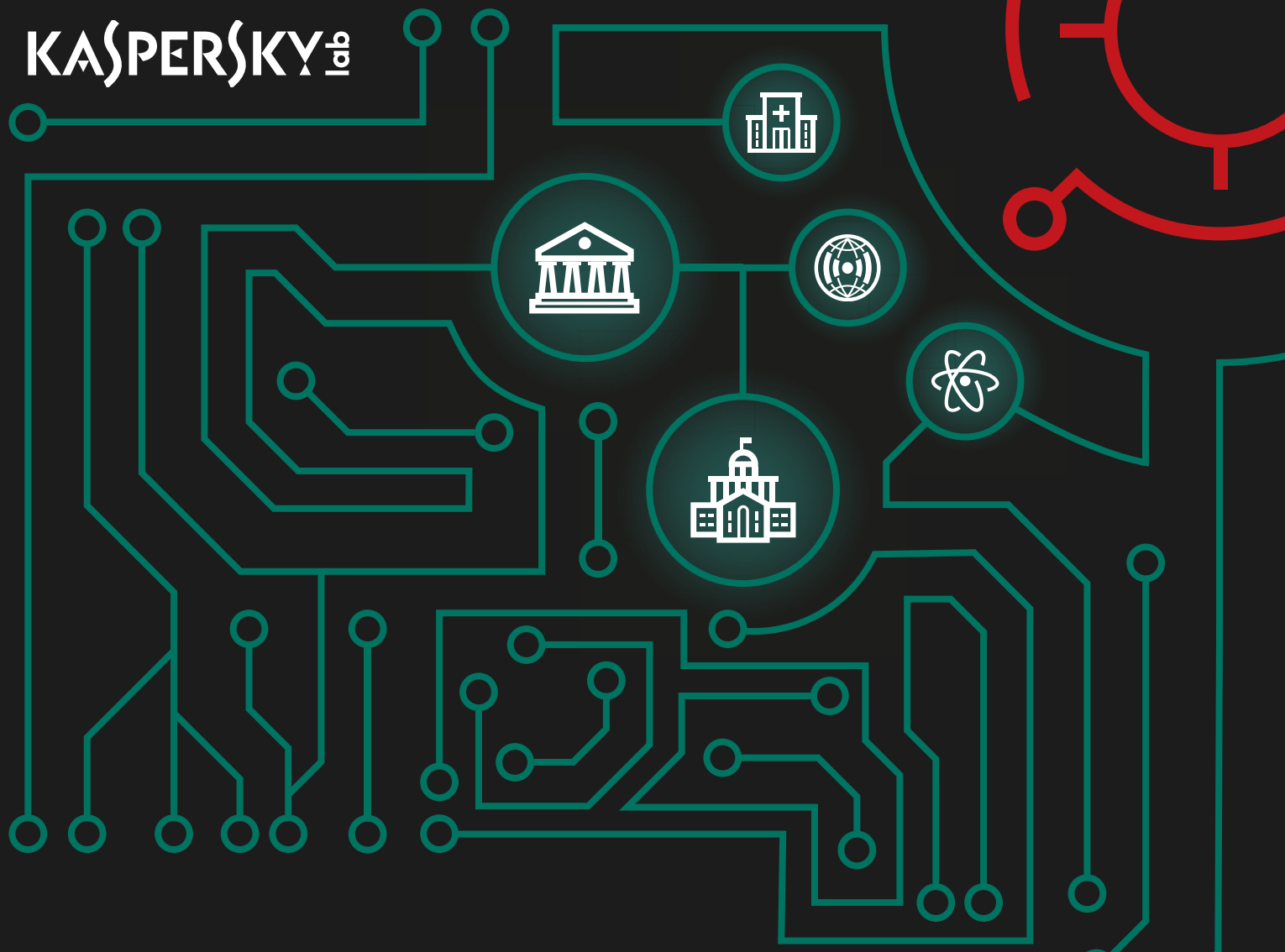
KASPERSKY lab



Kaspersky Security Bulletin:

2017. Сюжет года

СОДЕРЖАНИЕ

ШИФРОВАЛЬЩИКИ АТАКУЮТ

ВВЕДЕНИЕ: ЧТО НОВОГО МЫ УЗНАЛИ В 2017 ГОДУ

В 2017 году программы-вымогатели неожиданно развернулись в полную силу. Три беспрецедентные по силе и размаху кампании изменили ландшафт троянцев-вымогателей – причем, похоже, навсегда. Атаки были нацелены на бизнес, использовали для своего распространения червей и недавно попавшие в сеть эксплойты, шифровали данные и требовали выкуп, который на самом деле им был не нужен. Организаторы этих атак вряд ли являются рядовыми ворами, обычно стоящими за программами-вымогателями. Как минимум одна из атак содержала ошибки, позволяющие предположить, что преступники поторопились с ее запуском, другая распространялась через зараженное ПО для бизнеса. Две атаки из трёх были связаны между собой, а две самые крупные атаки были предназначены для уничтожения данных. Эти три атаки уже обошлись жертвам в сотни миллионов долларов.

Добро пожаловать в мир программ-вымогателей-2017. В уходящем году в постоянно растущем списке жертв этих зловредов к отдельным пользователям добавились крупные глобальные компании и промышленные системы, а злоумышленники, организующие целевые атаки, начали проявлять к шифровальщикам серьезный интерес. Этот год также отличается стабильно высокими показателями количества подобных атак при относительно небольшом проценте новых угроз.

Ниже приведен краткий анализ ключевых событий года.

КРУПНЫЕ АТАКИ – НЕ ТО, ЧЕМ КАЖУТСЯ

WannaCry

Все началось 12 мая, когда сообщество экспертов по кибербезопасности наблюдало явление, с которым не сталкивалось почти десять лет: кибератаку с использованием червя, который распространялся неудержимо. На этот раз червь был разработан для установки на зараженные компьютеры криптовымогателя WannaCry 2.0.

Эпидемия WannaCry затронула сотни тысяч компьютеров по всему миру. Для распространения червь использовал эксплойт под названием EternalBlue и бэкдор DoublePulsar – оба были опубликованы группой Shadow Brokers за месяц до начала атаки. Червь автоматически атаковал все компьютеры, находящиеся в одной локальной подсети с зараженной машиной, а также случайные диапазоны IP-адресов за пределами локальной сети, быстро распространяясь по земному шару.

Для заражения компьютера WannaCry эксплуатировал уязвимость в реализации протокола SMB в ОС Windows. Microsoft выпустила обновление для исправления этой уязвимости еще в марте 2017 года, но количество машин, на которых оно не было установлено, оказалось столь велико, что эта защитная мера не смогла помешать распространению WannaCry.

После заражения компьютера и выполнения действий, необходимых для дальнейшего распространения, WannaCry зашифровывал принадлежащие жертве ценные файлы и выводил на экран сообщение с требованием выкупа. Полная расшифровка файлов без выплаты выкупа была невозможна, хотя наши аналитики обнаружили в коде WannaCry несколько ошибок, которые в ряде случаев позволили жертвам восстановить некоторые свои данные без уплаты денег злоумышленникам.

Последствия эпидемии WannaCry

Атака не ограничилась какой-то одной отраслью: от нее в значительной мере пострадали различные организации с компьютерными системами, объединенным в сети. Также вымогатель поразил встроенные системы, которые зачастую работают на устаревших ОС и поэтому особенно уязвимы. Выкуп требовалось платить в биткойнах. По некоторым данным, в общей сложности жертвами WannaCry могли стать более 700 000 пользователей.

Автоконцерну Renault пришлось закрыть свой крупнейший завод во Франции, а больницы Великобритании вынуждены были отказывать в приеме пациентам. Также пострадали немецкий транспортный гигант Deutsche Bahn, испанская телекоммуникационная компания Telefónica, FedEx и другие. Даже спустя месяц после первой волны атаки WannaCry продолжал находить новые жертвы: так, Honda была вынуждена закрыть один из своих производственных объектов, а в штате Виктория, Австралия, пострадали 55 камер для контроля скорости передвижения.

WannaCry: вопросы без ответов

В качестве разрушительной масштабной атаки, нацеленной на предприятия и организации, WannaCry была чрезвычайно успешной. Но как атака программы-вымогателя с целью заработать много денег, WannaCry себя не оправдала. Распространение с помощью червя – не лучшее решение для угрозы, максимальный доход от которой можно получить, нападая на жертв исподтишка. По оценкам экспертов, из-за широкой огласки злоумышленникам удалось заработать на WannaCry всего лишь порядка 55 000 долларов в биткойн-эквиваленте. В коде имелись ошибки, на основании которых можно предположить, что троянец попал в «дикую среду» прежде, чем был полностью готов. Есть также ряд признаков, в том числе сходство с ранее известным кодом, позволяющих предположить, что группа, стоящая за WannaCry, – это печально известная корейскоязычная группировка Lazarus.

Истинная цель атаки WannaCry, возможно, никогда не будет известна: может быть, это была программа-вымогатель, с которой что-то пошло не так, или преднамеренная деструктивная атака, замаскированная под вымогательство.

ExPetr

Вторая крупная атака произошла спустя всего шесть недель, 27 июня. Она распространялась преимущественно посредством атаки на цепь поставок (supply-chain attack) и ее целью стали компьютеры, в основном в России, Украине и Европе. По данным телеметрии «Лаборатории Касперского», было атаковано более 5000 пользователей. Жертвы получали требование выкупа в размере 300 долларов, который необходимо было выплатить в биткойнах, хотя оказалось, что даже после этого они не смогли бы вернуть свои файлы.

ExPetr – сложная атака, включающая несколько векторов распространения. К ним относятся модифицированные эксплойты EternalBlue (также использованный WannaCry) и EternalRomance, бэкдор DoublePulsar для распространения по корпоративной сети, скомпрометированная программа для банковской отчетности MeDoc, которая распространяла вредоносное ПО через свои обновления, а для украинского региона Бахмут – зараженный новостной сайт, который был использован злоумышленниками для атаки типа watering hole.

Более того, ExPetr при определенных условиях мог распространяться на компьютеры с установленными необходимыми патчами, если они находились в одной локальной сети с зараженной машиной. Для этого он собирал учетные данные из зараженной системы с помощью инструмента, подобного Mimikatz, и распространялся далее по локальной сети при помощи PsExec и WMIC.

Компонент шифрования ExPetr работает на двух уровнях: зашифровывает файлы жертвы с помощью алгоритма AES-128, а затем устанавливает модифицированный загрузчик, взятый из другой вредоносной программы – GoldenEye (преемника Petya). Этот вредоносный загрузчик зашифровывает MFT (критически важную структуру файловой системы NTFS) и блокирует дальнейший процесс загрузки, требуя выкуп.

Последствия атаки ExPetr

Среди жертв ExPetr – крупные организации, в том числе порты погрузки, супермаркеты, рекламные агентства и юридические фирмы, например Maersk, FedEx (TNT) и WPP. Даже спустя месяц после атаки по-прежнему была нарушена работа службы доставки TNT, при этом особенно пострадали SMB-клиенты компании. Жертвой ExPetr также стал один из крупнейших производителей потребительских товаров Reckitt Benckiser – в течение 45 минут после начала атаки компания потеряла доступ к 15 000 ноутбуков, 2000 серверов и 500 компьютерным системам, и оценивает причиненный ущерб более чем в 130 миллионов долларов. Maersk объявила, что для нее потери дохода, вызванные этой атакой, составили около 300 миллионов долларов.

ExPetr: вопросы без ответов

Эксперты «Лаборатории Касперского» нашли сходство между ExPetr и ранними вариантами KillDisk (компонента BlackEnergy), но истинные мотивы и цель ExPetr также остаются неизвестными.

BadRabbit

В конце октября появился еще один крипто-червь – BadRabbit. Зловред начал распространяться с помощью drive-by-атаки, запускаемой с нескольких взломанных сайтов, и маскировался под обновление для Adobe Flash Player. При запуске на компьютере жертвы компонент BadRabbit с функционалом червя пытался распространяться с помощью эксплойта EternalRomance и применял тот же метод распространения по корпоративной сети, что и ExPetr. Большинство жертв BadRabbit находились в России, Украине, Турции и Германии.

Ransomware-компонент BadRabbit зашифровывал файлы жертвы, а затем и целые разделы диска, используя модули легитимной программы DiskCryptor. Анализ кода образцов и методов, используемых BadRabbit, показывает заметное сходство между этим вредоносным ПО и ExPetr. Однако, в отличие от ExPetr, BadRabbit не является вайпером и дает злоумышленникам технические возможности для дешифровки компьютера жертвы.

ПОПАВШИЕ В СЕТЬ ЭКСПЛОЙТЫ СПРОВОЦИРОВАЛИ НОВЫЕ ВОЛНЫ АТАК

Преступники, стоящие за вышеупомянутыми программами-вымогателями, были не единственными, кто использовал код эксплойтов, «слитых» группировкой Shadow Brokers, для проведения атак.

Мы обнаружили другие, не столь известные семейства шифровальщиков, которые использовали те же эксплойты. К ним относятся AES-NI (Trojan-Ransom.Win32.AecHu) и Uiwix (вариант Trojan-Ransom.Win32.Cryptoff). Эти семейства являются «чистыми» программами-вымогателями: они не обладают функционалом червя, то есть не могут самовоспроизводиться, поэтому и не получили такого широкого распространения, как, например, WannaCry. Тем не менее, преступники, стоящие за ними, использовали для первичного заражения те же самые уязвимости на компьютерах жертв.

ОПУБЛИКОВАНЫ МАСТЕР-КЛЮЧИ ДЛЯ НЕСКОЛЬКИХ СЕМЕЙСТВ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Помимо потрясших мир крупномасштабных эпидемий, во втором квартале 2017 года возникла интересная тенденция: несколько криминальных групп, стоящих за разными шифровальщиками-вымогателями, завершили свою деятельность и опубликовали секретные ключи, необходимые для дешифрования файлов жертв.

Ниже приведен список семейств, ключи для которых стали доступны во втором квартале:

- Crysis (Trojan-Ransom.Win32.Crusis);
- AES-NI (Trojan-Ransom.Win32.AecHu);
- xdata (Trojan-Ransom.Win32.AecHu);
- Petya/Mischa/GoldenEye (Trojan-Ransom.Win32.Petr).

Мастер-ключ для Petya/Mischa/GoldenEye был выпущен вскоре после массового распространения шифровальщика ExPetr. Возможно, это была попытка авторов Petya показать всем, что к ExPetr они отношения не имеют.

ВОЗВРАЩЕНИЕ CRYSIS

Несмотря на то, что вымогатель Crysis, казалось бы, прекратил свое существование в мае 2017 года после публикации всех мастер-ключей, выяснилось, что радоваться еще рано. В августе мы стали находить многочисленные новые образцы этого шифровальщика – почти точные копии распространявшихся ранее образцов, но с некоторыми отличиями: у них были новые мастер-ключи, новые адреса электронной почты, по которым жертвы должны были связываться со злоумышленниками, и новые расширения для зашифрованных файлов. Все прочее осталось неизменным, даже временные метки в PE-заголовках. После тщательного анализа старых и новых образцов наши аналитики пришли к выводу, что, скорее всего, новые образцы были созданы путем исправления двоичного кода старых с помощью hex-редактора. Возможно, преступники, стоящие за новыми образцами, не имели доступа к исходному коду и просто использовали реверс-инжиниринг, чтобы воскресить Crysis из мертвых и использовать его в своих целях.

ЧИСЛО ЗАРАЖЕНИЙ С ПОМОЩЬЮ RDP ПРОДОЛЖАЕТ РАСТИ

В 2016 году мы заметили новую тенденцию в методах «доставки» наиболее распространенных программ-вымогателей. Вместо того, чтобы использовать наборы эксплойтов или пытаться обманом вынудить жертву запустить вредоносный исполняемый файл, преступники сменили вектор атаки. Они осуществляют подбор логинов и паролей RDP на компьютерах, доступных из Интернета по RDP-протоколу.

В 2017 году этот подход стал одним из основных методов распространения нескольких семейств, таких как Crysis, Purgen/GlobeImposter и Cryakl. Это означает, что специалисты по IT-безопасности должны постоянно помнить об этом векторе атак и блокировать внешний доступ к корпоративной сети по RDP-протоколу.

ПРОГРАММЫ-ВЫМОГАТЕЛИ: ЦИФРЫ ГОДА

Важно не делать далеко идущие выводы из абсолютных цифр статистики, поскольку они отражают изменения не только в ситуации с угрозами, но и в методах их обнаружения. Учитывая это, можно отметить несколько важнейших тенденций года:

Степень новизны угроз снижается: в 2017 году 38 новых шифровальщиков (по сравнению с 62 в 2016 году) были признаны интересными и оригинальными настолько, чтобы претендовать на звание новых отдельных семейств в классификации. Это может объясняться тем, что модель атак с применением шифровальщиков имеет свои ограничения, и разработчикам вредоносного ПО становится все труднее изобретать что-то новое.

В 2017 году было обнаружено много модификаций новых и известных программ-вымогателей – более 96 000 по сравнению с 54 000 в 2016 году. Рост количества модификаций может быть вызван попытками обфускации кода программ-вымогателей со стороны злоумышленников, поскольку защитные решения стали обнаруживать это вредоносное ПО более успешно.

По данным, поступившим от пользователей продуктов «Лаборатории Касперского», в течение года количество атак оставалось более или менее постоянным. На смену резким всплескам, которые наблюдались в 2016 году, пришло более ровное распределение интенсивности атак по месяцам. В целом в 2017 году нападению подверглись около 950 000 уникальных пользователей, тогда как в 2016 году их было порядка 1,5 млн. Однако эти цифры включают и шифровальщиков, и их загрузчиков. Если же оценивать данные только по шифровщикам, количество атак в 2017 году будет примерно таким же, как и в 2016 году. Это может быть связано с тем, что многие злоумышленники начали использовать для распространения своих программ-вымогателей другие средства, например взлом паролей и ручной запуск. Эти цифры не учитывают множество не защищенных нашими решениями компьютеров по всему миру, которые стали жертвами WannaCry; их количество оценивается примерно в 727 000 уникальных IP-адресов.

Несмотря на WannaCry, ExPetr и BadRabbit, количество атак, нацеленных на компании и организации, возросло незначительно: с 22,6% в 2016 году до 26,2% в 2017. Только чуть более

Более подробную информацию об этих тенденциях, в том числе сведения о наиболее пострадавших странах, а также о наиболее популярных семействах вымогателей, можно найти в ежегодном отчете Kaspersky Security Bulletin 2017. Статистика.

4% атакованных в 2017 году компаний относились к сегменту малого и среднего бизнеса.

По данным ежегодного опроса по IT-безопасности, проводимого «Лабораторией Касперского»:

- 65% компаний, пострадавших от программ-вымогателей в 2017 году, сообщили, что потеряли доступ к значительному объему или даже ко всем своим данным. 29% организаций утверждают, что, хотя они и смогли расшифровать свои данные, значительное количество файлов было безвозвратно утрачено. Эти цифры во многом совпадают с данными 2016 года.
- 34% предприятий потребовалось неделя или даже больше, чтобы полностью восстановить доступ (29% в 2016 году).
- 36% жертв заплатили выкуп, но 17% из них так и не смогли восстановить свои данные (32 и 19% в 2016 году соответственно).

ЗАКЛЮЧЕНИЕ: ЧТО ЖДЕТ КРИПТОВЫМОГАТЕЛЕЙ?

В 2017 году криптовымогатели использовались злоумышленниками в ходе атак, по-видимому предназначенных для уничтожения данных, а не для получения финансовой выгоды. Число атак на домашних пользователей, малые и средние компании и крупные предприятия оставалось высоким, но в этих атаках применялся в основном существующий или модифицированный код вредоносных программ из известных или generic-семейств.

Означает ли это, что бизнес-модель криптовымогателей исчерпала себя? Существует ли более выгодная альтернатива для киберпреступников, ищущих финансовую выгоду? Одной из таких возможностей может быть майнинг криптовалют. Согласно прогнозам «Лаборатории Касперского» для криптовалют, в 2018 году вырастет количество целевых атак, задачей которых будет установка майнеров. В то время как программы-вымогатели дают потенциально большой, но единовременный доход, майнеры обеспечивают менее высокие, но более продолжительные заработки, и это может быть привлекательным для многих злоумышленников в современной изменчивой ситуации с троянцами-вымогателями. Одно можно сказать точно: вымогатели никуда не денутся - ни сами по себе, ни в качестве маскировки для более серьезных атак.

БОРЬБА С ВЫМОГАТЕЛЯМИ ПРОДОЛЖАЕТСЯ

С помощью сотрудничества: 25 июля 2016 года «Лаборатория Касперского», Национальная полиция Нидерландов, Европол и McAfee инициировали совместный проект No More Ransom. Это уникальный пример эффективного сотрудничества частных и государственных структур как в борьбе с киберпреступниками, так и в оказании помощи их жертвам – знаниями и опытом, советами и инструментами дешифрования. Год спустя в проекте, который теперь доступен на 26 языках, уже участвуют 109 партнеров. На онлайн-портале размещены 54 дешифратора, в целом охватывающих 104 семейства вымогателей. На сегодняшний день разблокировано более 28 000 устройств, в результате чего киберпреступники лишились примерно $9,5 млн. дохода.

С помощью информации: «Лаборатория Касперского» с самого начала отслеживала ситуацию с криптовымогателями, и одной из первых стала предоставлять постоянно обновляемые данные о них, чтобы повысить уровень осведомленности об этой угрозе в отрасли. Компания публикует регулярные обзоры развития ситуации, например, здесь и здесь.

С помощью технологий: «Лаборатория Касперского» предлагает многоуровневую защиту от этой широко распространенной и постоянно растущей угрозы, в том числе бесплатный инструмент для защиты от криптовымогателей, который любой желающий может скачать и использовать, независимо от уже установленного защитного решения. Продукты компании включают в себя еще один уровень защиты – модуль «Мониторинг активности», который может блокировать и откатывать вредоносные изменения, сделанные на устройстве, такие как шифрование файлов или блокировка доступа к монитору.

KASPERSKY lab