Storagenews (storagenews.ru), Москва, 21 июля 2017

ESET: ЗАЩИТА ОТ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

(Алексей Оськин -Руководитель отдела технического маркетинга ESET Russia)

Киберпреступники используют шифраторы и другие программы-вымогатели, чтобы ограничивать доступ пользователей к личным файлам на компьютерах или мобильных устройствах и требовать выкуп за его восстановление. Как правило, для заражения машины потенциальной жертвы используется фишинг или уязвимости программного обеспечения.

Среди известных шифраторов для ПК - Petya, WannaCry, Reveton, CryptoLocker, CryptoWall и TeslaCrypt; для мобильных платформ - Simplocker и LockerPin.

Как отмечают эксперты ESET, шифраторы являются популярным инструментом заработка в среде киберпреступников. Вымогатели используют в атаках на компании и на обычных пользователей. Чаще атаки нацелены на операционные системы Microsoft Windows и Google Android, хотя Linux и macOS тоже не застрахованы от шифраторов.

Как работают шифраторы

Вредоносные программы шифруют файлы наиболее распространенных типов на устройстве жертвы, а затем выводят на экран требование выкупа за ключ расшифровки. Иногда такая программа имеет встроенный таймер с заданным периодом времени для перевода выкупа.

Шифраторы активно распространяются в различных регионах мира. Стандартная схема заражения - рассылка писем, содержащих вредоносный файл в приложении или ссылку. " Качественные " фишинговые сообщения выглядят достаточно убедительно - их оформление и тексты копируют официальные информационные рассылки ведомств или компаний (Почта России, крупные банки или Налоговая служба, DHL и другие организации).

Злоумышленник легко определяет нахождение своих потенциальных жертв по домену верхнего уровня в электронном адресе пользователя или по домену интернет-провайдера. Когда пользователь открывает вложение или переходит по фишинговой ссылке в письме, на его компьютер устанавливается троянская программа, если, конечно, ее не блокирует антивирус. Далее троян-загрузчик устанавливает шифратор, который, в свою очередь, выбирает " знакомые " типы файлов для обработки. Современные шифраторы распознают десятки типов файлов распространенных форматов (.wma,.mov,.jpeg,.jpg,.rar,.zip,.ppt,.xls,.doc и др.) на жестких, съемных и сетевых дисках, затем шифруют найденное и выводят на экран сообщение для пользователя - инструкции по выплате выкупа. Сумма выкупа варьируется от психологически приемлемых 100-300 долларов до бесконечности.

В частности, троян-шифратор WannaCry (WannaCryptor, Wcry) требовал за восстановление доступа 300 долларов в биткоин-эквиваленте. Прибыль злоумышленников на момент наблюдений вирусной лаборатории ESET достигла 80 тысяч долларов - сравнительно небольшая сумма, в отличие от ущерба, который атака нанесла пользователям.

Предотвращение заражения

По данным опроса компании ISACA с участием 3000 специалистов по ИТ и ИБ, каждая пятая организация сталкивалась с заражением шифраторами. Риски корпоративного сектора особенно велики - в отличие от домашних пользователей, утрата доступа к критически важным ресурсам влечет потерю активов, включая объекты интеллектуальной собственности, репутационные убытки, снижение производительности и вынужденные простои в работе. Реальный финансовый ущерб от нарушений системы безопасности, связанных с вирусным заражением, с трудом поддается исчислению.

Авторы шифраторов используют продвинутые алгоритмы шифрования, по сложности зачастую превосходящие банковские механизмы защиты платежей клиентов. Восстановить данные после заражения современным шифратором затруднительно, а иногда и невозможно. Кроме того, обработанные шифратором файлы могут быть восстановлены некорректно.

Как следствие, дешевле принять меры предосторожности, чем расплачиваться за последствия заражения. Если корпоративные устройства не защищены, а сотрудники не обучены, ценные данные на ПК, мобильных устройствах и сетевых дисках могут быть потеряны навсегда.

Справедливо и обратное. Подготовительные работы для защиты системы минимизируют риск потери ценных данных. Чтобы снизить риски, рекомендуем выполнить следующие действия:

Используйте современные средства защиты

Заражение нередко происходит из-за устаревшего ПО, поэтому установите последнюю версию решения для защиты. Например, продукты ESET шестого поколения поддерживают новые эвристические технологии защиты от вредоносных программ, включая шифраторы. В их числе расширенное сканирование памяти, модуль " Защита от эксплойтов ", облачная система защиты, модуль " Защита от сетевых атак " и модуль " Защита от ботнетов ".

В частности, продукты ESET защищали от атак WannaCry еще до того, как шифратор был добавлен в вирусные базы. Модуль " Защита от сетевых атак " распознавал попытки атак с использования эксплойта EternalBlue, а эвристические технологии ESET блокировали угрозу на основе поведенческого анализа.

Узнать больше о продуктах ESET и их настройке против шифраторов вы можете на специальной странице - noransom. esetnod 32. ru .

Создайте резервную копию данных и регулярно ее обновляйте

Первая и лучшая мера защиты от шифраторов - регулярно обновляемая резервная копия данных. Помните, что вредоносные программы могут зашифровать файлы на всех видах сетевых дисков, включая облачные хранилища. Настройте автоматическое обновление резервных копий, а также не забывайте вручную обновлять копии на внешних дисках и в сервисах резервного копирования, которые могут быть отключены.

Регулярно устанавливайте патчи и обновления вашего ПО

Киберпреступники нередко рассчитывают на то, что пользователи игнорируют обновления программ и используют ПО с известными уязвимостями. Авторы вредоносных программ используют эти " дыры " в защите для незаметного вторжения в систему. Вы можете снизить риск атаки, если будете своевременно устанавливать обновления. Некоторые компании-разработчики ПО выпускают обновления регулярно. Не стоит игнорировать также внеплановые и срочные обновления. Включите автоматическое обновление ПО, если это возможно, либо скачивайте и устанавливайте обновления с сайтов разработчиков.

Простая рекомендация, однако эпидемия WannaCry показала, как много пользователей игнорирует базовые меры защиты. Шифратор распространялся в связке с эксплойтом EternalBlue для сетевой уязвимости Microsoft Windows. Microsoft выпустила обновление безопасности MS17-010, закрывающее данную уязвимость, еще 14 марта. Тем не менее, на момент начала атаки - 12 мая - патч был установлен далеко не на всех рабочих станциях, что обусловило массовый характер заражения.

Уделяйте внимание повышению грамотности сотрудников в вопросах информационной безопасности

Одним из наиболее распространенных способов заражения компьютеров является социальная инженерия. Злоумышленники вводят пользователей в заблуждение и убеждают открыть письмо, перейти по ссылке, запустить исполняемый файл - в общем, выполнить любое целевое действие. Важно обучать сотрудников компании и предостерегать их от открытия вложений и перехода по ссылкам в подозрительных письмах.

К сожалению, по данным собственного опроса ESET Russia, 69% респондентов никогда не проходили обучение основам информационной безопасности на своей работе. Еще 15% опрошенных сообщили, что курс обучения не выходил за рамки банальной рекомендации перезагрузить компьютер в случае неполадок. Только 16% респондентов прошли качественные тренинги.

Настройте отображение расширений файлов

Шифратор обычно содержится в файлах с расширением ".PDF" и ".EXE". Вредоносная программа рассчитывает на скрытие расширений файлов в ОС Windows, которое настроено по умолчанию. Включите отображение полного расширения файлов - это может облегчить обнаружение подозрительных файлов.

Настройте фильтр EXE-файлов в почте

Если ваш сканер почтовых шлюзов может фильтровать файлы по их расширениям в почте, настройте блокировку писем с вложенными EXE-файлами или файлами с двумя расширениями вида "*.*.EXE". Если вашим сотрудникам по роду деятельности необходимо обмениваться исполняемыми файлами, а вы установили фильтр на их пересылку, предложите создавать защищенные паролем ZIP-архивы или воспользоваться сервисами для обмена файлами. Рекомендуется также фильтровать файлы с расширениями: *.BAT, *.CMD, *.SCR и *.JS.

Отключите возможность запуска файлов из папок AppData или LocalAppData

Характерное для шифратора поведение напоминает работу исполняемого файла из папок AppData или Local AppData. Вы можете создать правила блокировки запуска исполняемых файлов для этих папок при помощи стандартных возможностей Windows или настроек HIPS в антивирусе. Если легальное приложение требует использовать для установки папку AppData вместо Program Files, вы можете сделать для него исключение.

Не забывайте про общие папки

Любое корпоративное устройство, зараженное шифратором, может спровоцировать шифрование всех файлов в общих папках, к которым имеет право на запись. Сотрудникам стоит задуматься, какие ценные и конфиденциальные данные они хранят на общих дисках. Их данные могут быть зашифрованными, даже если их персональный компьютер не был заражен.

Отключите возможности удаленного управления рабочим столом (RDP)

Чтобы попасть на компьютер, шифраторы часто используют RDP (протокол удаленного рабочего стола) - стандартную утилиту Windows для удаленного доступа. Также известно, что киберпреступники иногда получают доступ к целевой машине через RDP и отключают защитное ПО. Продукты ESET имеют встроенные механизмы самозащиты, однако мы рекомендуем отключить RDP, если вы не используете эту функцию.

Используйте программы для защиты, которым можно доверять

Киберпреступники обновляют свои вредоносные программы во избежание обнаружения, поэтому важно иметь многоуровневую защиту. После установки программа-вымогатель может атаковать не сразу, а только после получения удаленной команды. Даже если вредоносная программа абсолютно новая и " умеет " обходить антивирусное ПО, ее можно детектировать при попытке связаться с управляющим сервером. Новейшие версии продуктов ESET имеют встроенный модуль " Защита от ботнетов ", блокирующий несанкционированное внешнее " общение " программ.

Используйте восстановление системы, чтобы откатить систему до " чистого " состояния

Если на зараженном компьютере с установленной ОС Windows включена возможность восстановления системы, можно попробовать откатить систему до " чистого " состояния и восстановить часть зашифрованных файлов, используя теневые копии Windows. Для успешной операции нужно действовать быстро. Новейшие версии шифраторов могут удалять теневые копии для восстановления системы каждый раз, когда исполняемый файл запускается. Исполняемые файлы могут запускаться без участия оператора, как и обычные файлы при работе системы Windows.

Используйте стандартную учетную запись вместо учетной записи администратора

Когда вы используете учетную запись с правами администратора, вы подвергаете систему риску заражения, так как в этом случае вредоносные программы будут запускаться с повышенным уровнем прав. Убедитесь, что пользователи имеют учетные записи с ограниченными правами для выполнения своих ежедневных рабочих задач. Давайте права администратора только тем пользователям, которым это действительно необходимо. Не отключайте контроль учетных записей пользователей.

Платить или не платить?

Мы не рекомендуем платить выкуп вымогателям.

Во-первых, выкуп не обязывает злоумышленников дешифровать ваши данные или разблокировать устройства.

Если вы получили ключ для дешифровки, не факт, что он сработает. Нередки случаи, когда злоумышленники присылают неработающий или работающий частично ключ. Бывает, что PIN-код от зараженного Android-устройства не отправляется вымогателям, и они не могут разблокировать устройство при всем желании.

Во-вторых, заплатив выкуп, вы фактически спонсируете продолжение вредоносной деятельности.

В-третьих, а вы уверены, что вымогатели, получив выкуп, не вернутся вновь? Атака удалась, следовательно, они вполне могут снова использовать уязвимости вашей сети.

Если подозрительный файл уже запущен, и открытие некоторых файлов невозможно, немедленно отключите устройство от интернета и корпоративной сети. Это помешает вредоносной программе связаться с удаленным командным сервером до того, как она завершит шифрование данных на устройстве и подключенных дисках. Метод не гарантирует стопроцентной эффективности, но дает шанс спасти хотя бы часть файлов, прежде чем они будут полностью зашифрованы.

Если шифратор уже сделал свое дело, а у вас нет функциональной резервной копии, свяжитесь с технической поддержкой поставщика ваших антивирусных решений и проконсультируйтесь о дальнейших шагах по нейтрализации угрозы.

Учтите, что авторы вредоносного кода старались создать эффективный шифратор, используя продвинутые методы шифрования. Зачастую дешифровка невозможна или занимает много времени. Эксперты компании ESET стараются найти лазейки во вредоносной программе, которые позволяют исправить повреждения, нанесенные дискам и устройствам. По опыту, положительный результат достигается в одном случае заражения из пяти. Поиск уязвимостей в шифраторе занимает несколько недель или больше - все зависит от навыков авторов вредоносной программы. Не исключено, что дешифровать данные не удастся.

Рекомендуем заранее думать о защите важных данных, не дожидаясь пока шифратор придет к вам.

http://www.storagenews.ru/news_take.asp?Code=3864