АНТИВИРУСНАЯ ЗАЩИТА
БИЗНЕС-КЛАССА

ВИРУСЫ–ШИФРАТОРЫ И ПРОГРАММЫ–ВЫМОГАТЕЛИ

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Киберпреступники используют шифраторы и программы-вымогатели, чтобы ограничивать доступ пользователей к личным файлам на компьютерах или мобильных устройствах и требовать выкуп за его восстановление. Злоумышленники заражают устройства потенциальных жертв, используя фишинг и уязвимости программного обеспечения.

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

По оценкам ESET, шифраторы востребованы в среде киберпреступников. Эти программы используются в атаках как на компании, так и на обычных пользователей. Чаще атаки нацелены на операционные системы Microsoft Windows и Google Android, хотя Linux и Mac OS X тоже не застрахованы от шифраторов.

Чтобы помочь компаниям снизить риски, мы разработали рекомендации по защите корпоративных устройств и действиям в случае заражения. В документе представлен официальный ответ ESET на вопрос жертв шифраторов: «Платить или не платить?»

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. Когда жертва отправит платеж, а киберпреступник зафиксирует оплату, программа расшифровывает файлы. Если оплата не будет произведена, то это может привести к потере данных или даже поломке оборудования.

Программы-вымогатели могут заблокировать устройство и «взять в заложники» файлы, имеющие для вас особую ценность, личные или связанные с работой.

Вредоносное ПО обычно распространяется через электронные письма или вредоносные сайты (drive-by-download атаки). После установки на компьютер жертвы программа-вымогатель выводит на экран сообщение с требованием выкупа.

КАК РАСПРОСТРАНЯЮТСЯ ШИФРАТОРЫ

Шифраторы активно распространяются в масштабных киберкампаниях в различных регионах мира. Стандартная схема заражения – рассылка писем, содержащих вредоносный файл или ссылку. Потенциальная жертва может получить письмо на родном языке, подписанное известными местными компаниями. Например, злоумышленники нередко адресуют российским пользователям письма с вредоносным содержимым, подписанные Почтой России, Сбербанком или DHL. Такая тактика известна как фишинг.

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 осуществляет установку шифратора, который, в свою очередь, выбирает «знакомые» типы файлов для обработки. Когда шифрование завершено, программа выводит на экран сообщение для пользователя – требование о выкупе за «освобождение» файлов.

ОБНАРУЖЕНИЕ ШИФРАТОРОВ С ESET

Перед началом распространения вредоносных программ их авторы проверяют детектирование образцов статичными методами, используемыми в известных антивирусных продуктах. Следовательно, эффективная защита пользователя должна быть многоуровневой – сочетать технологии проактивной защиты, поведенческого анализа и облачных технологий.

Антивирусные решения ESET поддерживают несколько уровней защиты, включая технологии проактивного эвристического и реактивного обнаружения. Чтобы мгновенно реагировать на угрозы и обеспечивать максимальную защиту, антивирус должен быть обновлен и содержать актуальную информацию о последних обнаруженных угрозах, а облачный сервис ESET LiveGrid с информацией о репутации файлов – включен. Мы настоятельно рекомендуем использовать последние версии антивируса для возможности применения модулей «Защита от эксплойтов», «Расширенное сканирование памяти» и других технологий, детектирующих вредоносные программы на разных этапах их выполнения.

Нельзя забывать, что антивирусные решения не могут заменить другие инструменты обеспечения информационной безопасности. Поэтому необходимо уделять внимание таким вопросам как своевременное обновление программного обеспечения, регулярное создание резервных копий, информирование пользователей о методах социальной инженерии.

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 равноценна финансовым и репутационным потерям.

Авторы шифраторов используют продвинутые алгоритмы шифрования, по сложности зачастую превосходящие используемые в банках для защиты платежей клиентов. Это делает задачу восстановления данных непростой, а иногда и невозможной.

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.

ЧТОБЫ ПРАВИЛЬНО НАСТРОИТЬ ВАШИ ПРОДУКТЫ ESET, СЛЕДУЙТЕ РЕКОМЕНДАЦИЯМ НИЖЕ:

1. **Используйте последнюю версию программы для защиты**

   Заражение нередко происходит из-за устаревшего ПО, поэтому установите последнюю версию решения для защиты. При наличии действующей лицензии ESET обновление до последней версии бесплатно. Если вы используете ESET Endpoint Security 3 или 4, рекомендуем обновить решение до последней версии шестого поколения бизнес-продуктов. Продукты ESET шестого поколения поддерживают новые технологии защиты от вредоносных программ, включая шифраторы. В их числе расширенное сканирование памяти и модуль «Защита от эксплойтов», контролирующий процессы и выявляющий типичное для эксплойтов поведение.

2. **Регулярно обновляйте антивирус ESET**

   Новые версии шифраторов выходят достаточно часто, поэтому важным аспектом защиты от данного семейства вредоносных программ является регулярное обновление сигнатурных баз антивируса. Продукты ESET проверяют наличие обновлений каждый час при наличии действующей лицензии и интернет-подключения.

3. **Включите сервис ESET LiveGrid.**

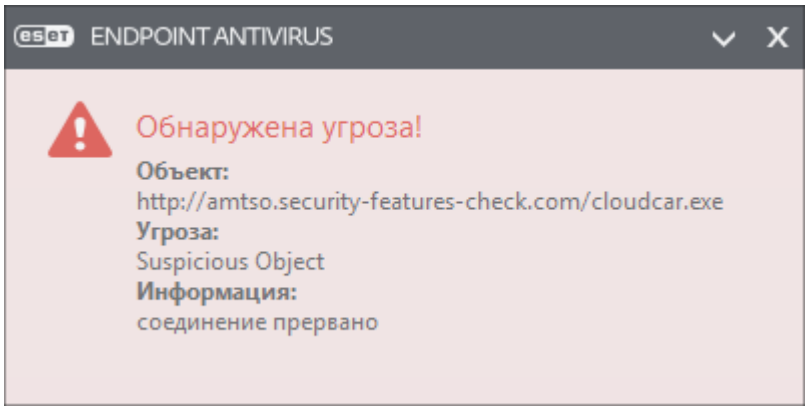
   С активированным облачным сервисом ESET LiveGrid антивирус реагирует на новые угрозы до того, как данное вредоносное ПО будет занесено

в сигнатурные базы, даже при условии их регулярного и максимально оперативного обновления. Собранные образцы неизвестных и потенциально опасных программ автоматически попадают в «песочницу» и подвергаются поведенческому анализу. При подтверждении вредоносного характера программы создаются автоматизированные сигнатуры. Клиенты ESET в считанные минуты узнают о новых угрозах благодаря сервису ESET LiveGrid – ждать обновления вирусных баз не требуется. Если процесс признан небезопасным, он немедленно блокируется. Важно отметить, что сервис ESET LiveGrid использует только хэш-функции подозрительных программ, соблюдая право пользователей на конфиденциальность.

Важная заметка

Брандмауэр вашей компании может заблокировать соединение с сервисом ESET LiveGrid, поэтому стоит убедиться, что он работает правильно. Посетите веб-страницу известной тестовой организации AMTSO, участником которой является ESET.

Нажмите на ссылку Download the CloudCar Testfile и скачайте файл cloudcar.exe. Если ESET LiveGrid работает правильно, файл откроется на серверах ESET и после получения необходимой информации будет блокироваться. При попытке загрузки появится следующее уведомление:



ПРОФИЛАКТИКА И ЗАЩИТА

Обработанные шифратором файлы могут быть некорректно восстановлены. Но если заранее провести подготовительные работы для защиты системы, риск потери данных будет значительно снижен. Для минимизации возможного влияния шифратора мы рекомендуем выполнить следующие действия:

11 ШАГОВ ДЛЯ ПРЕДОТВРАЩЕНИЯ ПОТЕРИ ДАННЫХ

1. Создайте резервную копию данных и регулярно ее обновляйте
2. Регулярно устанавливайте патчи и обновления вашего ПО
3. Уделяйте внимание повышению грамотности сотрудников в вопросах информационной безопасности
4. Настройте отображение расширений файлов
5. Настройте фильтр EXE-файлов в почте
6. Отключите возможность запуска файлов из папок AppData или LocalAppData
7. Не забывайте про общие папки
8. Отключите возможности удаленного управления рабочим столом (RDP)
9. Используйте программы для защиты, которым можно доверять
10. Используйте восстановление системы, чтобы откатить систему до «чистого» состояния
11. Используйте стандартную учетную запись вместо учетной записи администратора

1. Создайте резервную копию данных и регулярно ее обновляйте

Первая и лучшая мера защиты от шифраторов – регулярно обновляемая резервная копия данных. Помните, что эти вредоносные программы могут зашифровать файлы на всех видах сетевых дисков, в том числе в облачных хранилищах. Очень важно регулярно обновлять резервную копию. Настройте автоматическое обновление и не забывайте вручную обновлять копии на внешних дисках и в сервисах резервного копирования, которые могут быть отключены.

2. Регулярно устанавливайте патчи и обновления вашего ПО

Киберпреступники часто надеются на то, что пользователи не устанавливают последние обновления программ и используют устаревшее 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.

3. **Уделяйте внимание повышению грамотности сотрудников в вопросах информационной безопасности**

   Одним из наиболее распространенных способов заражения компьютеров является социальная инженерия – ее методы основаны на введении пользователей в заблуждение и убеждении их в том, что исполняемый файл необходимо запустить. Типичная схема заражения – открытие пользователем файла во вложении или переход по ссылке в письме или сообщении, которое он не запрашивал. Письмо может быть замаскировано под официальное сообщение банка, службы доставки и других доверенных организаций. Необходимо обучать сотрудников компании и предостерегать их от открытия вложений и перехода по ссылкам в подозрительных письмах.

4. **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.

5. **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.

6. **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.

7. **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

подвергаются риску быть зашифрованными, даже если их компьютер не был заражен.

8. **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.

9. **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 внешнее «общение» вредоносной программы.

10. **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.

11. **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.

КОМПЬЮТЕР УЖЕ ЗАРАЖЕН. ЧТО ДЕЛАТЬ?

Отключите устройство от 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, прежде чем 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.

Свяжитесь с технической поддержкой ESET

Если шифратор уже сделал свое дело, а у вас нет функциональной резервной копии, свяжитесь с технической поддержкой ESET. Вышлите специалистам логи антивируса (Сервис -> Файлы журнала -> клик правой клавишей мыши -> Экспортировать все или при помощи ESET Log Collector) и несколько образцов зашифрованных файлов (по возможности, около пяти документов Microsoft Word или Excel).

У вашей компании лицензия на сто и больше рабочих мест? Специалист техподдержки попросит больше информации о заражении. Далее наши эксперты совместно с вирусной лабораторией ESET в Братиславе попытаются восстановить пораженные файлы.

Имейте в виду, что авторы вредоносного кода старались создать эффективный шифратор, используя продвинутые методы шифрования. Зачастую дешифровка невозможна или занимает много времени.

Эксперты ESET постараются найти лазейки во вредоносной программе, которые позволят исправить повреждения, нанесенные дискам и устройствам. Если все пройдет успешно, вы получите инструмент для расшифровки.

Основываясь на нашем опыте, положительный результат достигается в одном случае заражения из пяти. Поиск лазейки в шифраторе занимает несколько недель или больше – все зависит от навыков авторов вредоносной программы. К сожалению, не исключено, что дешифрование будет невозможно.

ПОМНИТЕ ОБ ANDROID-УСТРОЙСТВАХ

Авторы вредоносных программ не ограничиваются платформой Microsoft Windows. В их поле зрения попала и *мобильная операционная система* Android, которая часто используется на корпоративных устройствах. Специалисты ESET изучили шифраторы, нацеленные на Android-устройства. Атакующие используют различные техники: создают фальшивые антивирусы, маскируют свои сообщения под уведомления правоохранительных органов (*Reveton*).

В 2014 году вирусные аналитики ESET обнаружили первый шифратор, *ориентированный на Android-устройства*. С тех пор появилось более 50 модификаций шифраторов, и новые опаснее предыдущих. В 2015 году появился первый вымогатель, блокирующий экран устройства случайным четырехзначным PIN-кодом.

Все эти программы могут перекрыть доступ к важным для бизнеса ресурсам и требовать выкуп за восстановление доступа.

КАК ЗАЩИТИТЬ ANDROID-УСТРОЙСТВА?

A) Обучите своих сотрудников

Сотрудники, использующие Android-устройства, должны знать о шифраторах и предпринимать меры предосторожности:

- избегать неофициальных или сторонних магазинов приложений;
- изучать отзывы других пользователей до того, как скачать приложение;
- проверять разрешения, которые запрашивает приложение при установке;
- загружать приложения из «белого списка», рекомендованного ИТ-службой компании.

B) Используйте антивирусные решения

Установите мобильное приложение для защиты и регулярно обновляйте его на корпоративных устройствах. Клиенты ESET могут использовать продукт ESET Endpoint Security для Android, входящий в состав следующих решений:

- ESET NOD32 Small Business Pack
- ESET NOS32 Antivirus Business Edition
- ESET NOD32 Smart Security Business Edition
- ESET NOD32 Secure Enterprise

C) Создайте резервную копию ценных файлов

Важно иметь функциональную резервную копию важных данных с каждого Android-устройства. Если пользователь принимает все меры предосторожности, шансы заражения шифратором стремятся к нулю. При наличии резервной копии заражение не повлечет никаких проблем.

МОБИЛЬНЫЕ УСТРОЙСТВА УЖЕ ЗАРАЖЕНЫ – ЧТО ДЕЛАТЬ?

Если корпоративное устройство заражено, есть несколько способов удаления вредоносной программы в зависимости от ее типа.

1. **Загрузите устройство в безопасном режиме**

   Если устройство заражено простым блокировщиком экрана, загрузка в безопасном режиме (когда сторонние приложения не загружаются) позволит удалить вредоносную программу. Способ перехода в безопасный режим зависит от настроек (эту информацию легко найти в руководстве пользователя или интернете).

2. **Отзовите права администратора у вредоносной программы**

   Если приложение получило права администратора (это характерно для программ-вымогателей), нужно отменить их в меню настроек до удаления приложения.

3. **Сбросьте пароль при помощи Mobile Device Manager**

   Ситуация усложняется, когда шифратор с правами администратора блокирует устройство, используя функциональные возможности встроенного PIN-кода или пароля от экрана блокировки. Должна быть предусмотрена возможность сброса пароля при помощи Android Device Manager или альтернативного MDM-решения. Для Android-устройств с root-правами есть еще больше возможностей.

4. **Свяжитесь с технической поддержкой**

   Если файлы зашифрованы такой программой как Android/Simplocker, лучше связаться с технической поддержкой ESET. Дешифровка возможна в зависимости от типа шифратора.

5. **Используйте сброс до заводских настроек**

   Сброс до заводских настроек, удаляющий все данные с устройства, используется как крайняя мера.

ПОСЛЕДНЕЕ, НО ОЧЕНЬ ВАЖНОЕ: ПЛАТИТЬ ИЛИ НЕ ПЛАТИТЬ?

ESET не рекомендует 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.

КРАТКИЕ ИНСТРУКЦИИ

Подводим итоги. Как защититься от шифратора?

До заражения

1. Создайте резервную копию данных и регулярно ее обновляйте
2. Регулярно устанавливайте патчи и обновления вашего ПО
3. Уделяйте внимание повышению грамотности сотрудников в вопросах информационной безопасности
4. Настройте отображение расширений файлов
5. Настройте фильтр EXE-файлов в почте
6. Отключите возможность запуска файлов из папок AppData или LocalAppData
7. Не забывайте про общие папки
8. Отключите возможности удаленного управления рабочим столом (RDP)
9. Используйте программы для защиты, которым можно доверять
10. Используйте восстановление системы, чтобы откатить систему до «чистого» состояния
11. Используйте стандартную учетную запись вместо учетной записи администратора

В случае подозрения на заражение

1. Отключите систему от интернета, если считаете, что компьютер был заражен
2. Обратитесь в техническую поддержку ESET для получения дальнейших инструкций:

- электронная почта: **support@esetnod32.ru**
- **8-800-200-01-57** (бесплатный номер по России)
- **8-10-800-200-01-57-1** (бесплатный номер для стран СНГ: Республика Беларусь, Казахстан, Киргизия, Молдавия, Таджикистан, Узбекистан)

3. И ни в коем случае не платите злоумышленникам!