Решения для бизнеса

KASPERSKY lab

WannaCry и другие шифровальщики: как обеспечить правильную защиту

www.kaspersky.ru

#ИстиннаяБезопасность

WannaCry и другие шифровальщики: как обеспечить правильную защиту

Многие, кто не сталкивался с шифровальщиками, – теперь в курсе, что это такое. В мае 2017 года организации по всему миру столкнулись с масштабной атакой вируса-шифровальщика WannaCry. Ему удалось зашифровать десятки тысяч компьютеров и нарушить работу сотен крупных организаций.

Атака подробно освещалась СМИ и вызвала широкий резонанс и у обычных пользователей, и у IT-специалистов. И все же, несмотря на масштаб поражения и медийную популярность WannaCry, надо признать, что эта атака является лишь логичным продолжением глобальной эпидемии шифровальщиков.

Количество программ-вымогателей, нацеленных как на бизнес, так и на обычных пользователей, стабильно растет все последние годы. Однако это не значит, что компании и обычные пользователи бессильны против этой угрозы. Регулярная профилактика и современные защитные решения способы справиться с шифровальщиками.

Как распространяется эпидемия

Информация об уязвимости
14 апреля
- Группировка Shadow Brokers опубликовала документ с данными об эксплойтах, якобы использующихся АНБ. В том числе он содержал упоминание об уязвимости, на которой решили «заработать» создатели шифровальщика.

Распространение
11 мая
- Вирус начинается распространяться.

12 мая
- Испанский CCS-CERT опубликовал предупреждение о заражении шифровальщиков нескольких организаций.
- Национальная служба Великобритании объявила о заражении 16 медицинских учреждений.
- Массовое заражение, начало эпидемии
- Вирус начинается распространяться с большой скоростью. Инфицированными оказались многие крупные предприятия и ведомства.
- Всего за один день «Лаборатория Касперского» зафиксировала 45 тысяч случаев атаки. Всего, по данным разных источников, заражению подверглись более 200 000 компьютеров.

Модификация
13-14 мая
- Появилось две заметных модификации шифровальщика, авторство которых, скорее всего, не принадлежит создателям оригинального вируса.

Спад эпидемии
15 мая
- Атака пошла на убыль. Количество попыток заражения снизилось в пять раз по сравнению с 12 мая. По данным Европола, атака затронула 150 стран по всему миру. Большинство атак пришлись на Россию. Также серьезно пострадали Украина, Тайвань, Индия.

Что такое WannaCry?

Это шифровальщик, эксплуатирующий сетевую уязвимость Microsoft Security Bulletin MS17-010. Microsoft выпустил обновление к ней еще 14 марта 2017 года, но к маю патч установили далеко не все компании. Воспользовавшись этим, киберпреступники получали удаленный доступ к компьютеру через эту уязвимость и устанавливали вредоносное ПО.

WannaCry отличается от большинства подобных вредоносных программ тем, что жертве не нужно было предпринимать никаких действий. Обычно, чтобы проникнуть ь в систему, кибепреступники применяют социальную инженерию, присылая по почте зараженные архивы или ссылки на поддельные сайты. Здесь можно было ничего не делать и все равно стать жертвой вируса.

После взлома WannaCry вел себя как червь: распространялся по локальной сети и шифровал компьютеры, на которых не был установлен патч. Шифрованию подверглись самые разные форматы файлов – в том числе офисные документы, архивы, файлы баз данных, файлы графических программ и фоторедакторов.

За расшифровку файлов киберпреступники требовали перечислить им выкуп в крипотовалюте Bitcoin – около 600 долларов США.

Рекомендации по защите

Рекомендации по защите от любого типа шифровальщиков просты:

- Регулярно создавайте резервные копии.
- Будьте осторожны с письмами – лучше не запускать подозрительные файлы и не переходить по ссылкам на незнакомые сайты.
- Ставьте патчи. Преступники постоянно ищут новые уязвимости в популярных программах (особенно страдает продукция Adobe и Microsoft). Их можно находить, приоритизировать и устанавливать автоматизированно – например, с помощью продукта Kaspersky Systems Management. Скажем, чтобы защититься от WannaCry, необходимо было установить официальный патч от Microsoft.
- Используйте надежное защитное решение. Если вы пользуетесь Kaspersky Security для бизнеса – убедитесь, что у вас включен компонент «Мониторинг системы».
- Не лишним будет ограничить активность программ, если ваше защитное решение это позволяет. Тогда вирус просто не сможет поразить всю сеть.

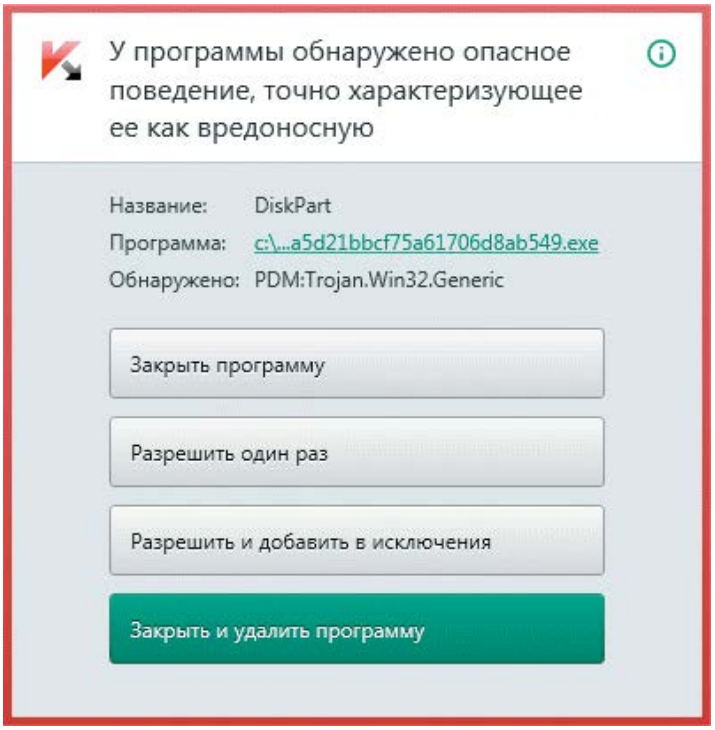
Какие технологии «Лаборатории Касперского» защищают от шифровальщиков?

Kaspersky Anti-Ransomware Tool

Бесплатная утилита, разработанная специально для защиты от шифровальщиков. Предназначена для пользователей и компаний, у которых не установлены продукты «Лаборатории Касперского». Работает параллельно с основным защитным решением.

Мониторинг системы

Модуль Kaspersky Security для бизнеса, который следит за активностью программ в системе и защищает от шифрования рабочие станции. Если он замечает подозрительное поведение, то позволяет завершить работу вредоносной программы и откатить все действия, которые она произвела.



Контроль запуска программ и Anti-Cryptor

Технология защиты серверов Anti-Cryptor защищает сервер от попыток шифрования с зараженного компьютера. Она автоматически блокирует доступ к серверу и останавливает процесс шифрования. Кроме того, с помощью правил можно разрешить или запретить запуск исполняемых файлов, скриптов или пакетов MSI, а также загрузку на сервер модулей DLL.

Расширенные инструменты системного администрирования

Kaspersky Security для бизнеса содержит инструменты патч-менеджмента, благодаря которым можно автоматически устанавливать обновления и исправления. При этом администратор видит, какие обновления нужно установить в первую очередь.

Kaspersky Security Network

Облачная база данных, которая в реальном времени распространяет информацию о новых угрозах. Если такая угроза зафиксирована, то защитные решения «Лаборатории Касперского» сразу же получают нужные вердикты, не дожидаясь обновления баз.

Максимальную защиту организаций от шифровальщиков обеспечивают Kaspersky Security для бизнеса Расширенный и Kaspersky Total Security для бизнеса.

Вопросы и ответы о шифровальщиках

WannaCry – это что-то из ряда вон выходящее?
С точки зрения масштаба заражения и поведения вируса – да. В то же время киберпреступники использовали стандартный способ внедрения в корпоративную сеть – уязвимости в Microsoft Windows. С точки зрения алгоритма шифрования (AES и RSA) — все тоже было стандартно.

Нужно ли устанавливать патчи, если у меня есть защитное решение?
Обязательно. Никто не гарантирует, что киберпреступники не используют эту уязвимость для атак другого типа – например, для кражи данных.

Я готов заплатить вымогателям, чтобы сохранить свои файлы. Почему нет?
Во-первых, киберпреступники могут просто получить деньги и не отдать вам ключ. Такое встречается довольно часто – в среднем, каждая пятая компания, которая платит выкуп, не получает ключа. Во-вторых, это мотивирует кибепреступников – раз их действия приносят деньги, они будут продолжать использовать шифровальщики.

У меня установлен антивирус. Мне угрожает шифровальщик?
Конечно, антивирус – это лучше, чем ничего. Однако против сложных угроз обычные антивирусы часто оказываются бессильны. В частности, для борьбы с шифровальщиками нужны продвинутые технологии, которые способны анализировать поведение объекта в системе. Впрочем, вы можете дополнить свой антивирус утилитой Kaspersky Anti-Ransomware Tool.

Пользователи Linux и Mac в безопасности?
Все относительно. WannaCry использовал уязвимость в Microsoft. Однако вирусы-шифровальщики под Linux и Mac тоже появляются, поэтому расслабляться не стоит.

Высокое качество защиты, подтвержденное независимыми тестами

Результаты тестирований, проведенных независимыми лабораториями AV-Comparatives и MRG Effitas, подтвердили, что флагманское решение «Лаборатории Касперского» Kaspersky Internet Security для всех устройств успешно защищало от атаки WannaCry еще до массового распространения шифровальщика.

Лаборатория MRG Effitas проверяла популярные решения кибербезопасности на защиту от эксплойта, который использовался для проникновения шифровальщика на устройство. С этой задачей справились лишь 3 из 14 тестируемых продуктов, среди которых Kaspersky Internet Security. Таким образом, это решение обеспечивает проактивную защиту на всех уровнях, чем может похвастаться лишь небольшое число программ.

Не менее эффективны в борьбе с троянцами-вымогателями продукты «Лаборатории Касперского» для бизнеса. Подтверждением этого стало еще одно тестирование MRG Effitas. Среди решений «Лаборатории Касперского» испытанию подверглись три: Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security Cloud и Kaspersky Anti-Ransomware Tool для бизнеса. Все они продемонстрировали 100% результат обнаружения и блокировки угроз и получили сертификат лаборатории.

Защита малого и среднего бизнеса

Kaspersky Small Office Security – комплексная защита малого бизнеса.

- Специализированная защита для малого и среднего бизнеса
- Защита финансовых операций с помощью технологии «Безопасные платежи»
- Защита мобильных устройств Android
- Облачная консоль мониторинга

Kaspersky Endpoint Security Cloud – надежная защита и удобная облачная консоль.

- Управление защитой из любой точки мира
- Предустановленные политики безопасности
- Безопасность мобильных устройств на всех популярных платформах
- Отсутствие затрат на покупку оборудования

Защита среднего и крупного бизнеса

Kaspersky Security для бизнеса Расширенный – многоуровневая защита от всех актуальных угроз.

- Оценка уязвимостей и автоматическая установка исправлений
- Шифрование всего диска или отдельных файлов
- Контроль запуска приложений на серверах
- Контроль использования программ, устройств и интернета

Kaspersky Total Security для бизнеса – комплексная безопасность IT-инфраструктуры на различных уровнях сети.

- Все инструменты уровня Расширенный, включая шифрование и патч-менеджмент
- Защита интернет-шлюзов
- Защита почтовых серверов
- Защита серверов совместной работы

www.kaspersky.ru

#ИстиннаяБезопасность