KASPERSKY lab

БОРЬБА С ШИФРОВАЛЬЩИКАМИ НА СЕРВЕРАХ И РАБОЧИХ СТАНЦИЯХ

www.kaspersky.ru

Программы-шифровальщики – один из самых быстрорастущих классов вредоносного ПО. Злоумышленникам не приходится даже похищать важные для бизнеса данные, чтобы кому-нибудь их продать: они просто зашифровывают их и требуют выкуп. Программы-шифровальщики эволюционировали из простых программ, блокировавших экран с требованием выкупа, однако теперь они куда опаснее. Особенно если вы не используете адекватную защиту от этого типа угроз.

ПОЧЕМУ ПРОГРАММЫ-ВЫМОГАТЕЛИ ТАК ОПАСНЫ

Программы-вымогатели основаны на крипторах – троянцах, которые проникают на компьютер через невинное на первый взгляд электронное письмо или ссылку на специально созданную интернет-страницу. Затем троянец незаметно шифрует все данные, которые может найти — например, финансовые документы или базы данных клиентов. За расшифровку файлов злоумышленники требуют выкуп, порой довольно значительный.

Естественно, что злоумышленники запутывают следы, поэтому они часто требуют оплаты в биткоинах и скрывают командные серверы в анонимной сети Tor. Если трафик между сервером и программой перехватывается, киберпреступники переходят к продвинутым криптографическим схемам, которые могут сделать расшифровку файлов невозможной. Все эти технологии были использованы, например, в атаках троянца Trojan-Ransom.Win32.Onion.

Сегодня многие шифровальщики требуют платежа не только за сами данные, но и за дополнительные «услуги». Например, преступники могут шантажировать людей, занимающих высокие должности: «Если не заплатишь, все узнают, какие сайты ты посещаешь».

ЭПИДЕМИЯ ШИФРОВАЛЬЩИКОВ

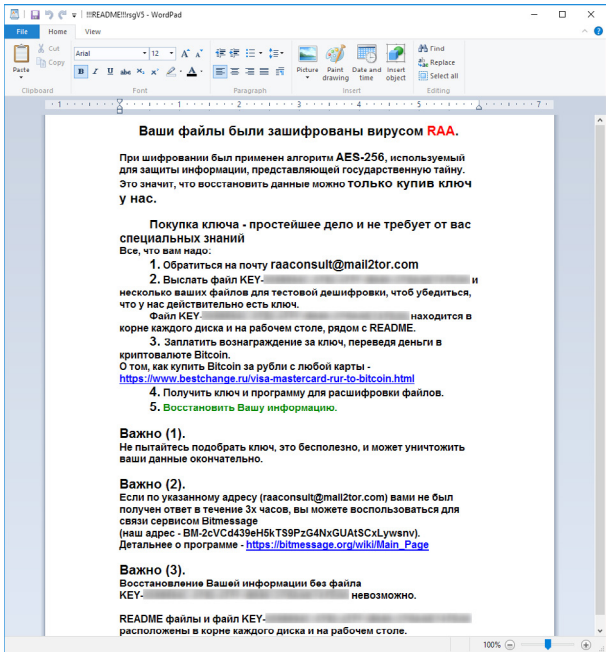
	Обнаружено шифровальщиков (через Kaspersky Security Network)
2014	121 238
2015	448430
Всего	**554 267**

В 2015 году общее число атак программ-шифровальщиков, зафиксированных Kaspersky Security Network, оказалось почти в четыре раза больше, чем годом ранее: в общей сложности **около 450 000**. Классификация шифровальщиков насчитывает множество типов и семейств – например, CryptoWall, TeslaCrypt, TorrentLocker и Locky. CTB-Locker, ACCDFISA и GpCode – только несколько примеров самых известных программ.

Locky – троянец, известный тем, что зашифровал данные медицинского центра в США. Первоначально Locky доставлялся на компьютеры жертв с помощью макросов в doc-файлах, но позже распространители таких программ стали также использовать zip-архивы с вредоносными скриптами.

TeslaCrypt: СМИ писали о TeslaCrypt как о «проклятии геймеров»: программа в первую очередь шифрует связанные с играми файлы (сохранения, пользовательские профили и так далее).

В 2016 года эпидемия стала еще масштабнее. Число шифровальщиков выросло в разы, появились множество новых видов таких программ. Отметим пару интересных экземпляров.



Petya — троянец, который попадает на компьютеры жертв с помощью электронного письма. В отличие от других вымогателей, он шифрует не отдельные типы файлов, а по сути весь жесткий диск с помощью шифрования главной таблицы файлов. Другая его особенность состоит в том, что эта программа работает без подключения к интернету.

RAA —шифровальщик, написанный на языке Jscript. В корпоративную сеть он попадает стандартным способом — с помощью письма, замаскированного под деловую переписку. К письму прикреплен zip-архив с паролем, чтобы стандартный антивирус не смог распознать вредоносное ПО. Интересно, что эта программа «в нагрузку» к шифрованию файлов запускает троянца Pony, созданного для кражи паролей.

КАК ЗАЩИЩАТЬСЯ

Несмотря на все сложные технологии, которые используют сегодняшние вредоносные программы, вред от них для вас и вашего бизнеса легко свести к минимуму. В частности, «Лаборатория Касперского» предлагает ряд средств защиты от программ-шифровальщиков.

Защитное решение должно быть включено абсолютно всегда, и в нем должно использоваться максимальное количество слоев защиты. Кроме того, решение должно регулярно обновляться.

Способов расшифровать файлы, испорченные современными шифровальщиками, пока не придумано, поэтому единственный способ спасти свои данные – это резервное копирование. Но все же одного резервного копирования (для которого можно использовать специальные решения, например программу Acronis) недостаточно: ведь оно не спасет недавно измененные файлы, а после восстановления система может снова стать жертвой шифровальщика.

Защита рабочих мест

«Лаборатория Касперского» разработала технологию Мониторинг системы (System Watcher). Расположенный на хосте, этот компонент защиты от вредоносного ПО анализирует все, что происходит с системой, в том числе изменение файлов. Обнаружив, что подозрительное приложение пытается открыть файлы, система сразу же создает локальную защищенную резервную копию. Если это приложение оказывается шифровальщиком (или другой вредоносной программой), Мониторинг системы автоматически откатывает нежелательные изменения. При этом эта функция не мешает работе пользователя и не требует от него никаких действий.

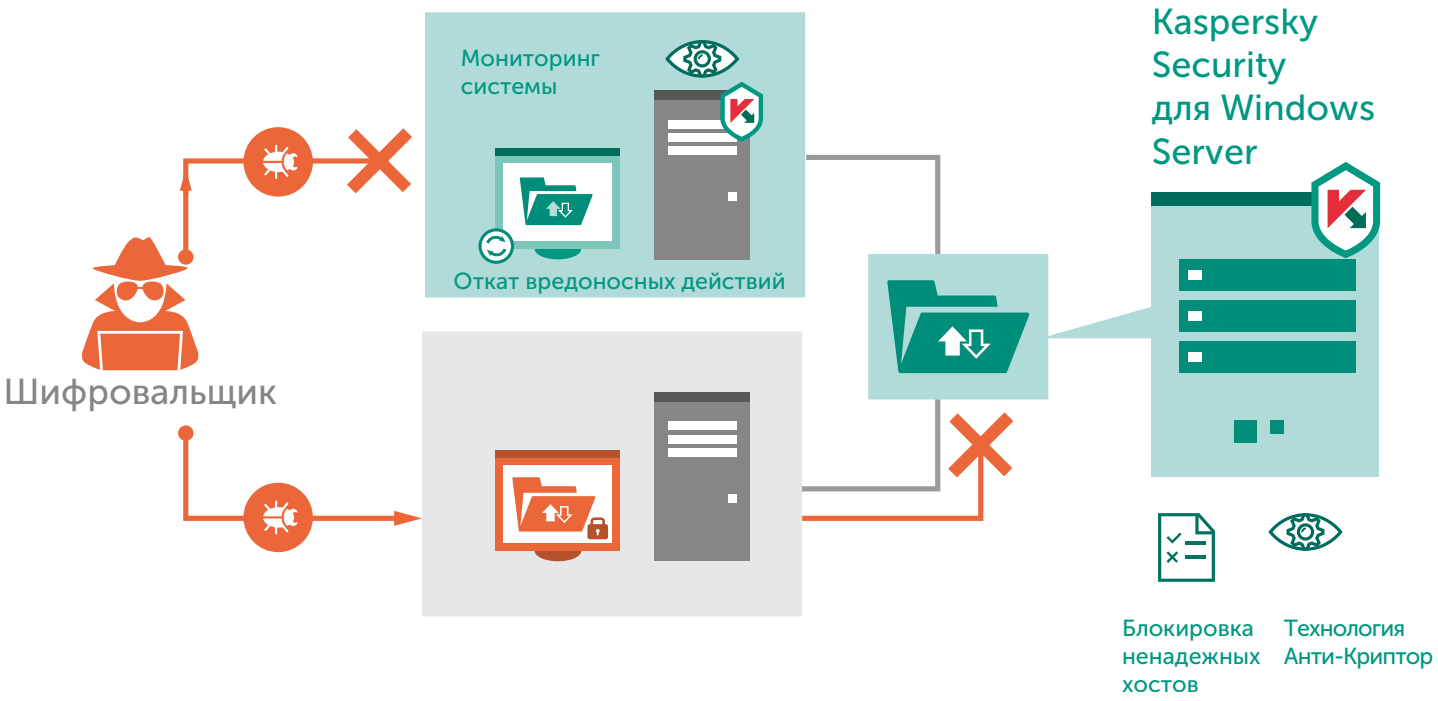
Мониторинг системы содержат все уровни решения Kaspersky Security для бизнеса, а также Kaspersky Endpoint Security Cloud.

Другая возможная защита от шифровальщиков – использовать контроль запуска программ с четкими правилами, не допускающими запуск неавторизованных программ.

Защита серверов

Некоторые компьютеры в периметре безопасности могут иметь папки SMB/CIFS на корпоративных серверах. И не на всех этих компьютерах всегда запущен компонент Мониторинг системы. На некоторых из этих компьютеров может не быть защитных программ, а решения, установленные на других, могут не обеспечивать защиту от шифровальщиков. В таком случае шифровальщик, проникнув на компьютер через письмо или уязвимость браузера, может зашифровать общие папки на корпоративных серверах. Единственная защита от этого – защитные решения для серверов.

Kaspersky Security для Windows Server предлагает новый уровень защиты, специально созданный для борьбы с шифровальщиками. Контроль над избранными папками, в том числе находящимися в общем доступе, позволяет сравнить состояние каждого файла до и после любой попытки доступа. Конечно, работа шифровальщика сильно изменит файл: он будет зашифрован! Поэтому этот механизм контроля почти всегда сможет обнаружить шифровальщика и заблокировать его дальнейшее развитие.



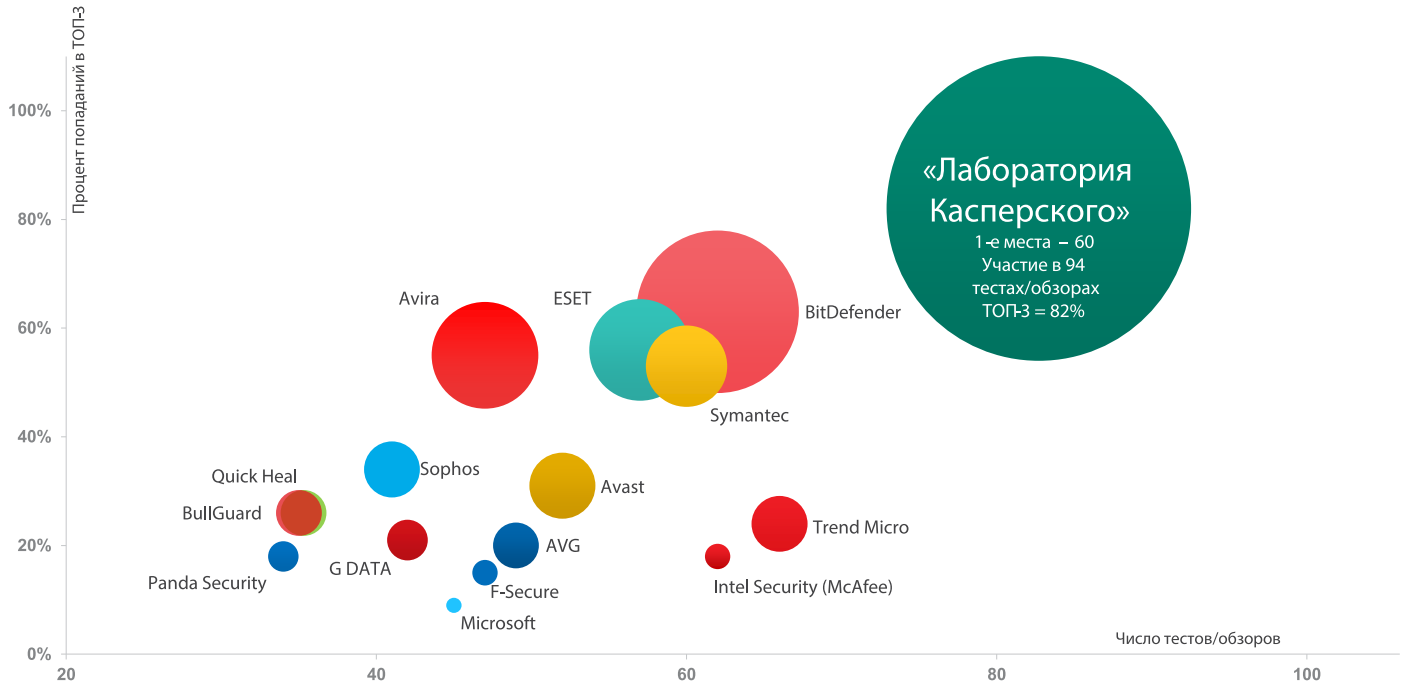
Шифрование папок на некоторых серверах может быть необходимо как часть периметра безопасности компании. Kaspersky Security для Windows Server позволяет администратору добавлять исключения для директорий, где используется такое шифрование.

Бескомпромиссная защита вашего бизнеса

Ландшафт угроз постоянно меняется, и «Лаборатория Касперского» делает все возможное, чтобы создать защиту от каждого нового поколения угроз и предложить надежное защитное решение. Мы помогаем клиентам снизить риски, связанные с шифровальщиками, как на рабочих станциях (Мониторинг системы), так и на серверах (Kaspersky Security для Windows Server).

«Лаборатория Касперского» постоянно обновляет свой арсенал технологий с помощью облачной системы глобальной аналитики.

Надежность решений «Лаборатории Касперского» для бизнеса подтверждена независимыми тестами. В 2015 году продукты «Лаборатории Касперского» приняли участие в 94 независимых тестах и обзорах. В 60 случаях они заняли первое место и 77 раз вошли в тройку лучших (ТОП-3).



Подробнее: www.kaspersky.ru/top3

Решения для защиты бизнеса:

kaspersky.ru/business