KASPERSKY lab

# ГОТОВ ЛИ ВАШ БИЗНЕС ОТРАЗИТЬ АТАКУ ШИФРОВАЛЬЩИКОВ?

*Узнайте, как защититься от шифрующих программ-вымогателей*

## Что такое программа-вымогатель?

**Давно миновали дни, когда вредоносные программы сочиняли любители «развлечений». Современные вредоносные программы создаются кибергруппировками, целью которых является похищение денег.**

Программа-вымогатель — это особый тип вредоносной программы, которая пытается получить выкуп в обмен на разблокирование доступа к тому или иному ресурсу жертвы.

В случае шифрующих программ-вымогателей в роли «заложников» оказываются файлы и данные, хранящиеся на зараженном устройстве. Такой шифровальщик кодирует данные жертвы, делая их нечитаемыми. Для раскодирования требуется ключ, который преступник сообщает только после выплаты выкупа.

Программа выводит на экран требование, согласно которому пользователю необходимо перевести деньги злоумышленникам за расшифровку содержимого устройства.

## Размер ущерба

**Программе-вымогателю совершенно не важно, частный ли вы пользователь, предприятие малого или среднего бизнеса, либо корпорация — задача киберпреступников заразить как можно больше систем.**

С пользователей киберпреступники обычно требуютвыкуп в размере от 300 долларов, но отлично понимают, насколько важными могут быть данные для бизнеса, и сумма выкупа с организаций, как правило, намного выше.

Заразив устройства, злоумышленник обычно дает жертве на уплату выкупа от 48 до 72 часов. Если деньги не заплатить в срок, то требуемая за расшифровку сумма может возрасти. Если после истечения повторного срока выкуп так и не будет получен, то ключ расшифровки удаляется, и вернуть файлы в читаемый вид уже нельзя.

Но даже если вы заплатите вымогателям, нет гарантии, что ваши данные будут расшифрованы. Некоторые вредоносные программы содержат ошибки, которые не позволяют правильно расшифровать файлы. В других случаях преступники, которые изначально не собирались заниматься расшифровкой, просто забирают у жертвы деньги.

**Более 40%** жертв CryptoLocker согласились выплатить выкуп[1].

Современная программа-шифровальщик часто препятствует восстановлению зашифрованных данных. В частности, удаляются или шифруются теневые копии, в которых хранятся точки восстановления системы и регулярно создаваемые резервные копии Windows.

Андрей Пожогин, эксперт по кибербезопасности, «Лаборатория Касперского»

*1: По данным проведенного в 2014 году исследования Центра междисциплинарных исследований в области кибербезопасности при Кентском университете.*

# Дополнительные убытки для организаций

**Преступники часто требуют с организаций повышенный выкуп, но сама по себе выплаченная сумма — это еще полбеды. Причиненные атакой неудобства могут обернуться куда большими финансовыми потерями.**

В сегодняшний информационный век даже кратковременная потеря данных может полностью нарушить течение важнейших бизнес-процессов, что влечет:

- **Репутационные риски**
- **Перебои в работе**
- **Снижение продаж**
- **Падение эффективности труда**
- **Значительные расходы на восстановление системы**

Если же потерянные данные не удастся восстановить, то последствия могут быть куда более суровыми:

- **Непоправимая утрата конкурентоспособности компании**
- **Падение выручки в долгосрочной перспективе**
- **Недоступность данных, составляющих интеллектуальную собственность, и данных для проектирования**

Более того, само существование организации может оказаться под угрозой.

Представьте, что вы лишились доступа ко всем сведениям о торговых операциях, клиентской базе, бухгалтерским отчетам, информации о продукции и данным для проектирования. Переживет ли ваш бизнес такой удар? Сколько прибыли вы не получите, пока будете приводить дела в порядок?

Очевидно, что любая организация должна делать все возможное, чтобы не стать жертвой программы-шифровальщика.

Если вы подверглись такой атаке, не прибегайте к популярным в интернете неофициальным «лекарствам». Такие программы лишь усугубят ваши проблемы:

**1**

**Часто они вовсе не работают, а лишь пытаются получить дополнительные деньги**

**2**

**Некоторые из них загружают в сеть жертвы новые вредоносные программы**

Неофициальное ПО из интернета, которое якобы может расшифровать зараженные данные, может быть опасным. В лучшем случае оно окажется просто бесполезным, а в худшем — заразит систему дополнительным вирусом.

Андрей Пожогин, эксперт по кибербезопасности, «Лаборатория Касперского»

# Активность шифровальщиков постоянно растет

**Разработать и запустить программу-шифровальщик сравнительно просто. Более того, полный исходный код некоторых программ шифровальщиков находится в открытом доступе для всех желающих. Всего одна версия такой программы приносит значительную прибыль, так что подобных атак становится все больше.**

Вот лишь ряд примеров современных шифровальщиков:

**CryptoLocker** заразил десятки тысяч компьютеров, принеся преступникам миллионы долларов.

**TorLocker** шифрует данные, а затем связывается с преступниками, организовавшими атаку, по сети Tor.

**Trojan-Ransom.AndroidOS.Pletor** – первый шифровальщик для Android.

**CoinVault** шифрует файлы жертв по алгоритму AES с 256-битным ключом.

**CryptoWall** часто удваивает сумму выкупа, если деньги не уплачиваются в требуемый срок.

**За первое полугодие 2015 года количество атак шифровальщиков сравнялось с их числом за весь 2014 год[1].**

Несмотря на распространение программ-вымогателей, лишь **40%** компаний считают их серьезной угрозой.

Такое отношение делает систему безопасности особенно уязвимой для киберпреступников[2].

*1: По данным Kaspersky Security Network.*

*2: Данные исследования «Информационная безопасность бизнеса», проведенного «Лабораторией Касперского» и B2B International в 2015 году. В исследовании приняли участие более 5500 IT-специалистов из 26 стран мира, включая Россию.*

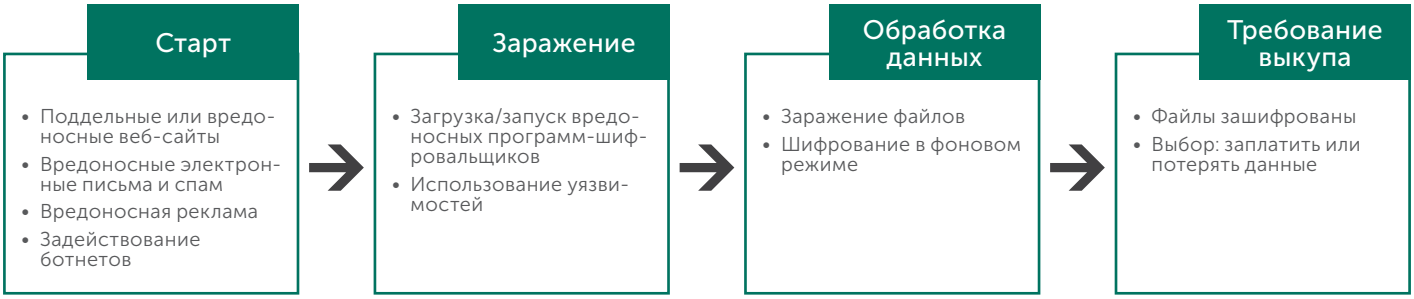
# Механизм атаки шифровальщика

**Как и большинство других типов вредоносного ПО, программа-шифровальщик может проникать на компьютеры и в другие устройства многими способами.**

Наиболее распространены следующие два.

- **Фишинговые письма или спам-рассылка**: жертва получает по электронной почте сообщение, которое содержит зараженное вложение или ссылку на фишинговый веб-сайт.
- **«Рассадники»**: устройство может оказаться зараженным после посещения легального (но недостаточно защищенного) сайта, популярного среди определенных групп пользователей (например, форума для бухгалтеров или сайта деловых консультаций). В подобных случаях веб-сайт с эксплойт-паками распространяет вредоносное ПО, нацеленное на уязвимости в устройствах посетителей.

# Стадии атаки




# Что атакуют шифровальщики

Стоит помнить, что программа-шифровальщик атакует очень разные устройства, в том числе:

- Компьютеры Windows®
- Компьютеры Mac®
- Планшеты и смартфоны Android™
- Инфраструктуру виртуальных рабочих столов (VDI)

Если атакованное устройство подключено к сетевому диску для доступа к корпоративным данным, то вредоносная программа зашифрует общие файлы на этом диске.

## Современные шифровальщики опаснее предшественников

**Разрушительный эффект первых шифровальщиков раньше часто удавалось устранить.**

Иногда ключ расшифровки хранился на зараженном устройстве, и нужно было только суметь его найти, чтобы расшифровать данные. В других случаях специалистам по безопасности удавалось вскрыть вредоносную программу и найти способ расшифровать данные, анализируя ее код.

Однако современные киберпреступники больше не совершают таких простых ошибок. Они применяют весьма изощренные технологии. Даже если удастся проникнуть в код шифровальщика, вряд ли вы найдете ключ шифрования на зараженном устройстве.

Сегодня шифровальщики создают уникальный ключ расшифровки для каждого атакованного устройства, который не позволяет расшифровывать файлы на других устройствах.

Наряду с такими технологиями используются все более сложные схемы шифрования, в том числе:

- **комбинированный метод RSA/AES** — данные шифруются на высокой скорости по алгоритму AES, а затем ключ AES шифруется стойким алгоритмом RSA;
- **алгоритмы на эллиптических кривых** — шифрование оказывается более стойким при сохранении скорости.

Все это делает расшифровку данных практически невозможной.

## Заметая следы

Киберпреступники, использующие программы-шифровальщики, прикладывают немало усилий, чтобы скрыться от правоохранительных органов. Современных кибервымогателей выследить и обезвредить нелегко.

- Как правило, выкуп требуется вносить в Bitcoin или другой электронной валюте, платеж в которой непросто проследить.
- Такие механизмы анонимизации, как сеть Tor, усложняют отслеживание местонахождения преступников.

# Как защитить бизнес

**На риск атаки шифровальщиков можно реагировать двумя способами:**

**1. Надеяться, что вы не станете жертвой атаки. Учитывая, с какой скоростью растет число шифровальщиков, этот вариант не выглядит реалистичным.**

**ИЛИ**

**2. Соблюдать ряд простых правил, которые сохранят безопасность ваших данных и рабочих процессов.**

*Регулярно создавайте резервные копии данных*
Практически во всех организациях существует требование резервного копирования данных. Однако важно, чтобы данные копировались в автономную резервную подсистему, а не просто хранились на одном из компьютеров корпоративной сети. Иначе преступники смогут зашифровать и резервные копии ваших файлов.

Следуйте правилу «скопировал и отключил», а не просто копируйте данные на постоянно подключенный к сети файловый сервер.

*Информируйте пользователей*
Самым уязвимым элементом любой организации часто оказываются ее сотрудники. Научите их основам IT-безопасности:

- Расскажите об опасностях фишинга, в том числе целевого (spear-phishing).
- Объясните, к чему приводит открытие подозрительных вложений электронной почты, даже полученных из доверенных источников.

*Защищайте все устройства и системы*
Поскольку шифровальщики атакуют не только компьютеры с Windows, ваше программное решение по безопасности также должно защищать компьютеры Mac, виртуальные машины и мобильные устройства Android.

Также следует уделить достаточное внимание защите почтовой системы.

*Установите защитные программы и поддерживайте их актуальность*
Главное оружие против любых вирусных атак – это быстрое и частое обновление, поэтому:

- **обновляйте все приложения и операционные системы**, чтобы устранить новые обнаруженные уязвимости.
- **обновляйте защитные программы и антивирусные базы**, чтобы получить самую актуальную защиту.

Подберите такое защитное решение, которое позволит:

- **управлять доступом к интернету** – например, в соответствии с занимаемой должностью;
- **управлять доступом к корпоративным данным** – опять-таки, в зависимости от должности или отдела;
- **управлять запуском программ** с помощью технологий Контроля программ, которые позволяют разрешать или блокировать те или иные программы.

Киберпреступники разрабатывают все более незаметные версии вредоносного ПО и пользуются множеством приемов, чтобы скрыть работу шифровальщика от жертвы.

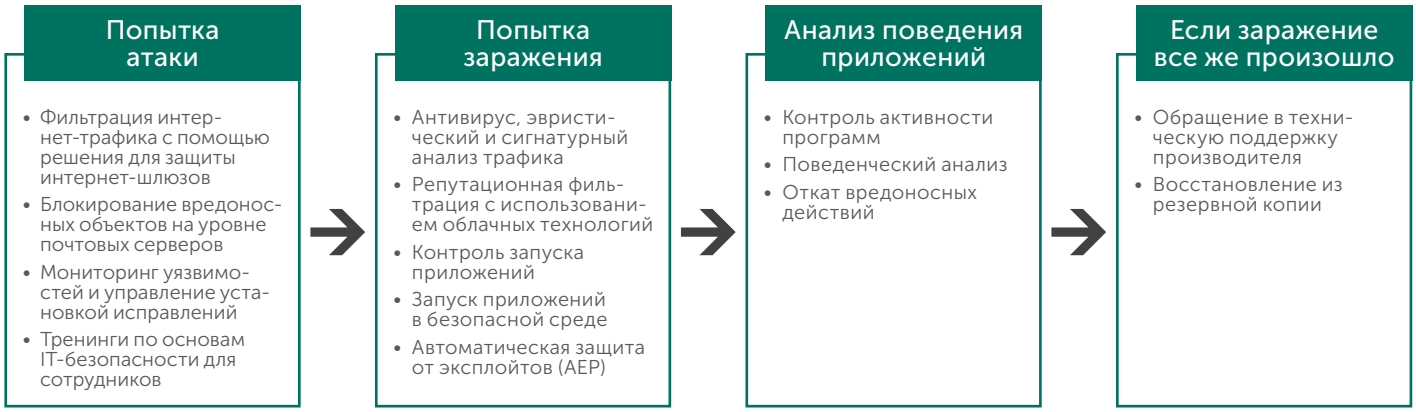
Андрей Пожогин, эксперт по кибербезопасности, «Лаборатория Касперского»

# Проверенная защита

**Kaspersky Endpoint Security для бизнеса обеспечивает многоуровневую защиту от известных, неизвестных и комплексных угроз, в том числе от шифровальщиков.**

**Наше защитное приложение и антивирусные базы обновляются чаще, чем у большинства других поставщиков решений безопасности. Кроме того, в Kaspersky Endpoint Security для бизнеса входят проактивные, эвристические и облачные технологии защиты, что позволяет особенно быстро реагировать на новые угрозы.**

**В состав многих наших продуктов также входят дополнительные защитные инструменты и технологии.[1]**




*Мониторинг системы с технологией противодействия программам-шифровальщикам*
Мониторинг системы следит за работой программ и сравнивает их поведение с моделями, характерными для вредоносного ПО.

Обнаружив подозрительную программу, Мониторинг системы автоматически помещает ее в карантин. Мониторинг системы также ведет динамический журнал операционной системы, реестра и других операций, что позволяет выполнять откат действий, совершенных вредоносной программой до ее обнаружения.

Кроме того, Мониторинг системы постоянно контролирует доступ к файлам, включая документы Microsoft Office, а при запросе доступа к ним сохраняет их временные копии. Если Мониторинг системы обнаружит, что к файлам обращался подозрительный процесс (например, шифровальщик), то временные резервные копии позволят вернуть файлы в незашифрованный вид. Временные резервные копии, создаваемые Мониторингом системы, не могут заменить резервное копирование данных, однако бывают полезны для устранения последствий атаки шифровальщика.

Контроль активности программ, работающий вместе с Мониторингом системы, также ограничивает доступ программ к критическим системным ресурсам, в том числе запрещает низкоуровневый доступ к диску.

*Мониторинг уязвимостей и управление установкой исправлений*
Уязвимости (особого рода ошибки) приложений и операционных систем открывают дорогу различным вредоносным программам, в том числе шифровальщикам.

Наши автоматические средства проверяют системы, обнаруживают и устраняют известные уязвимости и помогают в распространении необходимых обновлений и исправлений.

*Автоматическая защита от эксплойтов (AEP)*
Технология AEP препятствует проникновению вредоносного ПО через уязвимости в приложениях и операционных системах. Она следит за приложениями, которые чаще всего становятся мишенью для атак — Adobe® Reader, Internet Explorer®, Microsoft Office, Java™ и др., — и образует мощный дополнительный уровень безопасности.

*Защита файловых серверов*
Решение Kaspersky Security для файловых серверов защищает от шифрования папок для совместной работы. Если на какой-либо машине замечена подозрительная активность, приложение блокирует для нее доступ к общим сетевым ресурсам.

*1: Набор функций безопасности зависит от типа системы и платформы. Подробности см. на сайте www.kaspersky.ru/business*

Инновационные защитные продукты и технологии «Лаборатории Касперского» получили больше наград, чем предложения других поставщиков решений безопасности.

В 2015 году наши продукты завоевали **первое место** в 60 из 94 независимых тестов и обзоров.

**БОЛЬШЕ ТЕСТОВ***
**БОЛЬШЕ НАГРАД**
**БОЛЬШЕ ЗАЩИТЫ**

*kaspersky.com/top3

*Контроль программ и белые списки*
Гибкие средства Контроля программ и динамические белые списки позволяют легко разрешать или запрещать запуск программ. Помимо блокировки программ из черного списка, для некоторых рабочих станций и серверов можно ввести в действие режим «Запрет по умолчанию» и разрешить только программы из белого списка. В этом случае шифровальщики будут блокироваться автоматически.

*Веб-Контроль*
Удобные инструменты для настройки политик доступа к интернету и отслеживания использования интернета. Можно запрещать, разрешать или регистрировать действия пользователей на отдельных веб-сайтах или категориях сайтов (онлайн-игры, социальные сети, азартные игры и т. п.), чтобы уменьшить вероятность заражения.

*Антифишинг*
Наше облачное антифишинговое ядро защищает сотрудников от стандартного фишинга и целевых кампаний, которые приводят к заражению шифровальщиками.

*Защита почтовой системы*
Kaspersky Security для почтовых серверов проверяет входящую, исходящую и сохраненную почту на серверах Microsoft Exchange, Linux Mail и Lotus Domino. Современное облачное антиспам-ядро вместе с антифишинговым ядром помогает сотрудникам не отвлекаться на спам, а также обеспечивает защиту от шифровальщиков и других угроз.

*Защита рабочих мест[1] и не только*
«Лаборатория Касперского» предлагает решения для защиты самых разнообразных устройств:

- компьютеров Windows
- компьютеров Mac
- файловых серверов
- мобильных телефонов и планшетов
- виртуальных серверов
- инфраструктуры виртуальных рабочих столов (VDI)
- интернет-шлюзов
- серверов совместной работы

# О «ЛАБОРАТОРИИ КАСПЕРСКОГО»

«Лаборатория Касперского» — международная компания, работающая в сфере информационной безопасности с 1997 года. Глубокие экспертные знания и опыт компании лежат в основе защитных решений и сервисов, обеспечивающих безопасность бизнеса, критически важной инфраструктуры, государственных органов и пользователей во всем мире.

Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для широкого круга пользователей. «Лаборатория Касперского» защищает домашних пользователей, небольшие компании, предприятия среднего бизнеса и крупные корпорации от всевозможных киберугроз, предлагая всем при этом удобные инструменты для управления системой безопасности.

«Лаборатория Касперского» понимает потребности небольших компаний и предлагает им многоуровневые решения, эффективные и простые в управлении. Компания также отвечает всем запросам крупных предприятий, предоставляя им комплексную платформу, которая защищает от всех типов киберугроз, обнаруживает самые сложные атаки, реагирует на любые инциденты и предвидит развитие угроз. Кроме того, компания предлагает набор специализированных решений, которые защищают все узлы корпоративной сети, включая мобильные устройства, а также способны обеспечить безопасность центров обработки данных и индустриальных сред.

Решения для бизнеса: kaspersky.ru/business



KASPERSKY lab