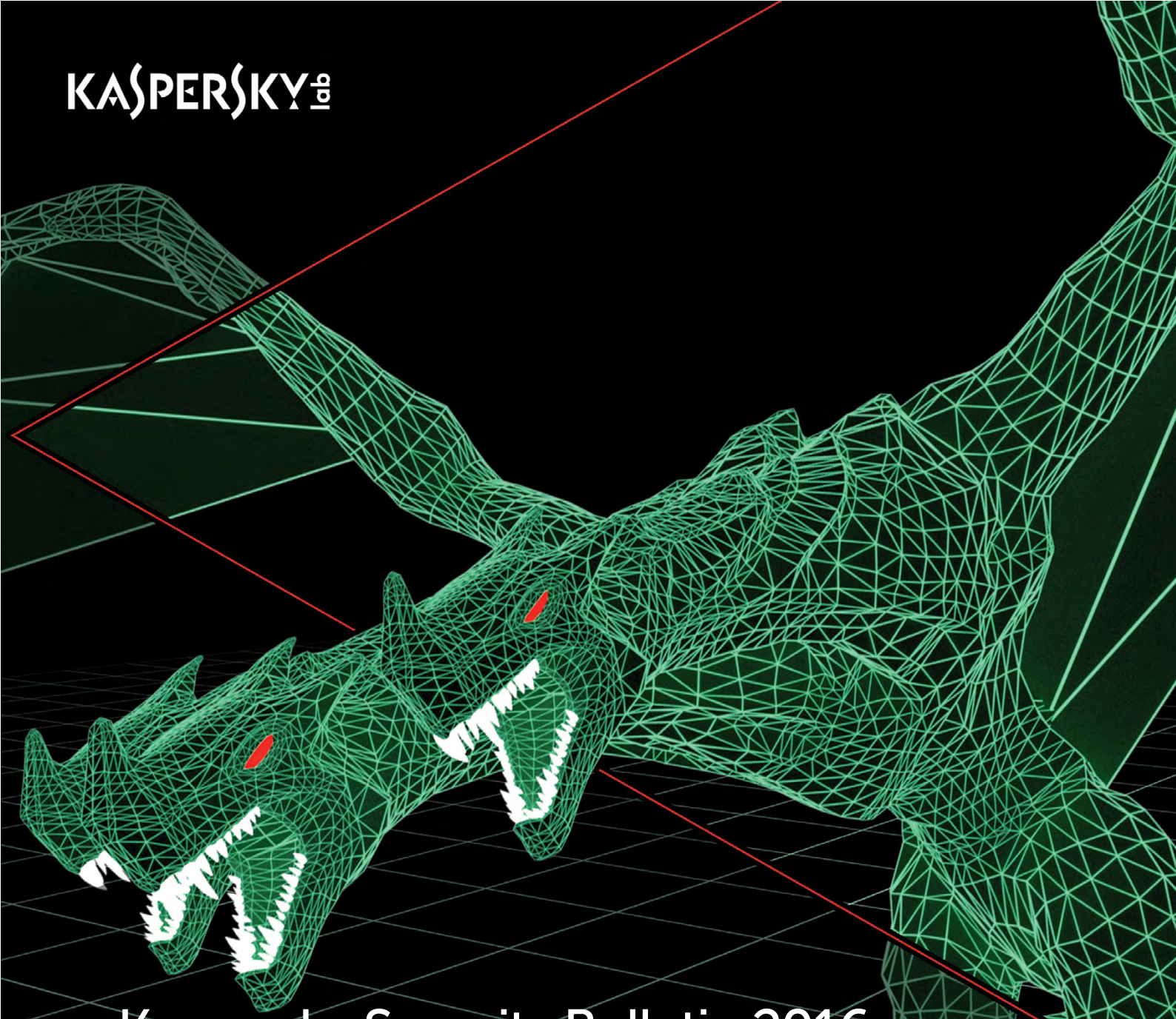
KASPERSKY lab



Kaspersky Security Bulletin 2016

СЮЖЕТ ГОДА. ПРОГРАММЫ-ВЫМОГАТЕЛИ: РЕВОЛЮЦИЯ

GREAT

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В 2016 году вредоносные программы-вымогатели продолжили завоевание мира, захватывая в плен данные и устройства как отдельных пользователей, так и целых компаний.

Цифры говорят сами за себя:

- Возникло 62 новых семейства программ-вымогателей.
- Количество новых модификаций вымогателей выросло в 11 раз — с 2900 в период с января по март до 32 091 в июле-сентябре.
- С января по конец сентября число атак на компании увеличилось в три раза: если в январе атаки проводились в среднем каждые две минуты, то в сентябре — уже каждые 40 секунд.
- Интенсивность атак на пользователей удвоилась: атаки проводились в среднем раз в 20 секунд в начале периода и раз в 10 секунд в его конце.
- Каждая пятая компания малого или среднего бизнеса, заплатившая выкуп, так и не получила доступ к своим данным.

В 2016 году наблюдался также рост сложности и разнообразия программ-вымогателей. Например, появились вымогатели, меняющие тактику при встрече с финансовым ПО; стало расти число вымогателей, написанных на скриптовых языках, вымогателей, использующих новые пути заражения, вымогателей, рассчитанных на отдельные группы пользователей, а также готовых решений типа «вымогатели как услуга» для тех, у кого недостаточно навыков, ресурсов или времени. Всё это происходит через расширяющуюся и всё более эффективную подпольную экосистему.

В то же время, в 2016 году в мире началось организованное противостояние вымогателям.

В июле был запущен проект No More Ransom, объединивший усилия Национальной полиции Нидерландов, Европола и компаний Intel Security и «Лаборатория Касперского»; в октябре к проекту присоединились ещё 13 организаций. Помимо прочих результатов, в рамках проекта в интернете было размещено несколько бесплатных утилит для расшифровки файлов; они уже помогли тысячам жертв восстановить данные, зашифрованные программами-вымогателями.

Наше сотрудничество в борьбе с программами-вымогателями только начинается, и многое ещё предстоит сделать. Вместе мы сможем добиться гораздо большего, чем каждый поодиночке.

Что такое программы-вымогатели?

Программы-вымогатели бывают двух видов. Самый распространенный — это шифровальщики. Они зашифровывают данные на устройстве пользователя и требуют денег (выкуп), взамен обещая восстановить данные. В отличие от них блокировщики не изменяют данные, а блокируют доступ пользователя к устройству, на котором эти данные хранятся. Требование о выкупе демонстрируется на экране устройства и, как правило, маскируется под сообщение от правоохранительных органов о том, что пользователь получил доступ к незаконному веб-контенту и должен немедленно заплатить штраф. Обзор обоих типов программ-вымогателей доступен здесь.

ПРОГРАММЫ-ВЫМОГАТЕЛИ: ОСНОВНЫЕ ТЕНДЕНЦИИ И ОТКРЫТИЯ 2016 ГОДА

«В большинстве случаев успех вымогателей строится на специфических доверительных отношениях между жертвой и атакующей стороной, которые подразумевают, что после получения выкупа злоумышленник вернет жертве ее файлы. Как ни удивительно, киберпреступники до сих пор демонстрировали некое подобие профессионализма в исполнении этого негласного обещания».

GReAT, Прогноз развития угроз на 2017 г.

Новые и выбывшие игроки

Новые зловреды. В 2016 году увидели свет Cerber, Locky, CryptXXX и ещё 44 287 новых модификаций программ-вымогателей

На сегодняшний день вымогатель Locky распространился по

114

странам мира

Cerber и Locky появились в начале весны. Оба зловреда являются вымогателями, опасными и широко распространившимися – в основном через вложения к спам-сообщениям и наборы эксплойтов. Оба, «работая» как с частными пользователями, так и с корпоративным сектором, быстро утвердились в качестве крупных игроков. Несильно от них отстал и вымогатель CryptXXX. Все три семейства продолжают развиваться, требуя выкуп за зашифрованные данные у пользователей по всему миру, наравне с такими известными вымогателями, как CTB-Locker, CryptoWall и Shade.

Наиболее распространенные семейства программ-вымогателей, детектируемые продуктами «Лаборатории Касперского», по состоянию на октябрь 2016 года:

	Название	Вердикты*	Доля пользователей**
1	CTB-Locker	Trojan-Ransom.Win32.Onion / Trojan-Ransom.NSIS.Onion	25,32%
2	Locky	Trojan-Ransom.Win32.Locky / Trojan-Dropper.JS.Locky	7,07%
3	TeslaCrypt (был активен до мая 2016 г.)	Trojan-Ransom.Win32.Bitman	6,54%
4	Scatter	Trojan-Ransom.Win32.Scatter / Trojan-Ransom.BAT.Scatter / Trojan-Downloader.JS.Scatter / Trojan-Dropper.JS.Scatter	2,85%
5	Cryakl	Trojan-Ransom.Win32.Cryakl	2,79%
6	CryptoWall	Trojan-Ransom.Win32.Cryptodef	2,36%
7	Shade	Trojan-Ransom.Win32.Shade	1,73%
8	(Generic-вердикт)	Trojan-Ransom.Win32.Snocry	1,26%
9	Crysis	Trojan-Ransom.Win32.Crusis	1,15%
10	Cryrar/ACCDFISA	Trojan-Ransom.Win32.Cryrar	0,90%

* Детектирующие вердикты продуктов «Лаборатории Касперского». Информация получена от пользователей продуктов «Лаборатории Касперского», давших свое согласие на передачу статистических данных.

** Процент пользователей, атакованных данным семейством шифровальщиков-вымогателей, от числа всех пользователей, атакованных шифровальщиками-вымогателями.

Выбывшие игроки – Teslascrypt, Chimera, Wildfire: не спеши говорить «до свиданья»...

Пожалуй, самой большой неожиданностью 2016 года стало отключение троянца-вымогателя TeslaCrypt и последующая публикация мастер-ключа к нему – видимо, самими владельцами зловреда.

TeslaCrypt «покончил с собой», а Encryptor RaaS и Wildfire были отключены полицией

Encryptor RaaS, один из первых троянцев, предлагавшихся вирусописателями другим киберпреступникам в рамках модели Ransomware-as-a-Service (вымогатель как услуга), прекратил свою активность после того, как полиция отключила часть его ботнета.

Затем, в июле некто, якобы имевший отношение к шифровальщику Petya/Mischa, опубликовал около 3500 ключей к вымогателю Chimera. Учитывая, что часть исходного кода Chimera была использована в Petya, вполне может быть, что за этими двумя вымогателями стоит одна и та же группировка, которая просто решила обновить свою продуктовую линейку и заодно покуражиться.

Похожая история произошла с вымогателем Wildfire — его командные серверы были отключены, а совместными усилиями «Лаборатории Касперского», Intel Security и Европола был создан ключ расшифровки. Однако теперь вымогатель, судя по всему, возродился под именем Hades.

«Учебные» вымогатели на службе у киберпреступников

Исследователи, действовавшие из лучших побуждений, создали «учебные» программы-вымогатели, чтобы дать системным администраторам инструмент моделирования атак с применением такого вредоносного ПО для целей тестирования защитных систем. Киберпреступники быстро приспособили эти инструменты для своих криминальных целей.

Из программ-вымогателей, созданных в «образовательных» целях, возникли, в частности, такие зловреды как Ded Cryptor и Fantom

Разработчик «учебного» вымогателя Hidden Tear & EDA2 из лучших побуждений опубликовал его исходный код на веб-сервисе GitHub. Не удивительно, что в 2016 году появилось множество троянцев, созданных на основе этого кода, в том числе вымогатель Ded Cryptor, который менял фон рабочего стола на зараженном компьютере на картинку со злобным Санта-Клаусом и требовал выкуп размером в два биткойна (около 1300$). Другой такой программой был Fantom, который маскировался под обновление Windows и показывал экран обновления, очень похожий на настоящий.

Нестандартные подходы

Злоумышленники теперь нацелились на резервные копии и жесткие диски, а также на подбор паролей

- **Зачем возиться с файлом, если можно зашифровать сразу весь диск?**

  В 2016 году возник такой новый подход в работе программ-вымогателей, как шифрование диска: эти зловреды блокируют доступ к диску или шифруют сразу все файлы на нем. В качестве примера можно привести троянскую программу Petya, которая шифрует главную файловую таблицу (master file table, MFT) жесткого диска и делает невозможной нормальную перезагрузку компьютера. Другой троянец, Dcryptor, также известный как Mamba, пошел еще на шаг дальше – он блокирует сразу весь жесткий диск. Это особенно неприятный вымогатель — он шифрует каждый сектор диска, включая операционную систему, приложения, файлы совместного использования и все личные данные, с помощью программы с открытым исходным кодом DiskCryptor.

- **Метод «ручного» заражения**

  Заражение троянцем Dcryptor происходит вручную — злоумышленники подбирают пароли, чтобы получить удаленный доступ к компьютеру-жертве. Подход не нов, но стал значительно более популярен в 2016 году; он часто используется для проведения атак на серверы и последующего проникновения в корпоративную сеть.

  В случае успешной атаки троянец устанавливается на сервере и шифрует файлы, которые хранятся на нем и, в некоторых случаях, на всех доступных с этого сервера сетевых ресурсах. Мы обнаружили, что данный подход применяется в троянце TeamXRat — с его помощью бразильские киберпреступники заражают программой-вымогателем бразильские сервера.

Обнаружив на компьютере финансовое ПО, Shade скачивал на него шпионскую программу

- **Заражение «два-в-одном»**

  В августе мы обнаружили образец Shade, у которого был неожиданный функционал: в случае, если зараженный компьютер имел отношение к департаменту финансов, троянец вместо стандартного шифрования файлов скачивал и устанавливал шпионскую программу, вероятно с более долгосрочной целью кражи денежных средств.

Вымогатели на скриптовых языках

Ещё один тренд 2016 года, на который мы обратили внимание, — это рост числа шифровальщиков, написанных на скриптовых языках. Только в третьем квартале мы обнаружили несколько новых семейств троянцев-вымогателей, написанных на Python, в их числе HolyCrypt и CryPy, а также Stampado, который написан на AutoIt — языке для автоматизации выполнения задач.

Армия киберпреступников-любителей и плагиаторов

Если программа-вымогатель плохого качества, то это увеличивает вероятность безвозвратной утери данных

Многие троянцы-вымогатели, впервые обнаруженные в 2016 году, оказались низкого качества — незамысловатые, с ошибками в коде и банальными описками в текстах требования выкупа.

Кроме того, мы заметили, что создатели программ-вымогателей копируют друг друга. В частности, мы обнаружили следующее:

- Троянец Bart копирует текст требования выкупа и стиль страницы уплаты выкупа у Locky.
- Написанный на AutoIt троянец-вымогатель, копирующий Locky (он получил название AutoLocky) использует то же расширение для зашифрованных файлов – ".locky".
- Crusis (он же Crysis) использует расширение ".xtbl", позаимствованное у Shade.
- Xorist полностью копирует схему именования зашифрованных файлов, используемую Crusis.

Из всех творений плагиаторов, обнаруженных в этом году, пальму первенства мы присуждаем Polyglot (он же MarsJoke). Этот троянец полностью копирует внешний вид CTB-Locker и его подход к обработке файлов.

Мы ожидаем, что все эти тенденции получат свое развитие в 2017 году.

«Программы-вымогатели становятся все более притягательными, привлекая менее квалифицированные слои киберпреступников. В результате в будущем мы будем все чаще сталкиваться с программами-вымогателями, за которыми стоят киберпреступники, не выполняющие вышеописанное молчаливое соглашение — из-за ошибок в коде или в силу того, что функционал восстановления файлов в программе просто не реализован. Мы ожидаем появления программ-вымогателей, созданных так называемыми «скрипт-кидди» (начинающими хакерами), которые будут блокировать файлы или доступ к системе или будут просто удалять файлы, обманным путем заставляя жертв платить, но при этом не возвращая им доступ к файлам».

GReAT, Прогноз развития угроз на 2017 г.

ПРОЦВЕТАЮЩАЯ ЭКОНОМИКА, ОСНОВАННАЯ НА ТРОЯНЦАХ-ШИФРОВАЛЬЩИКАХ

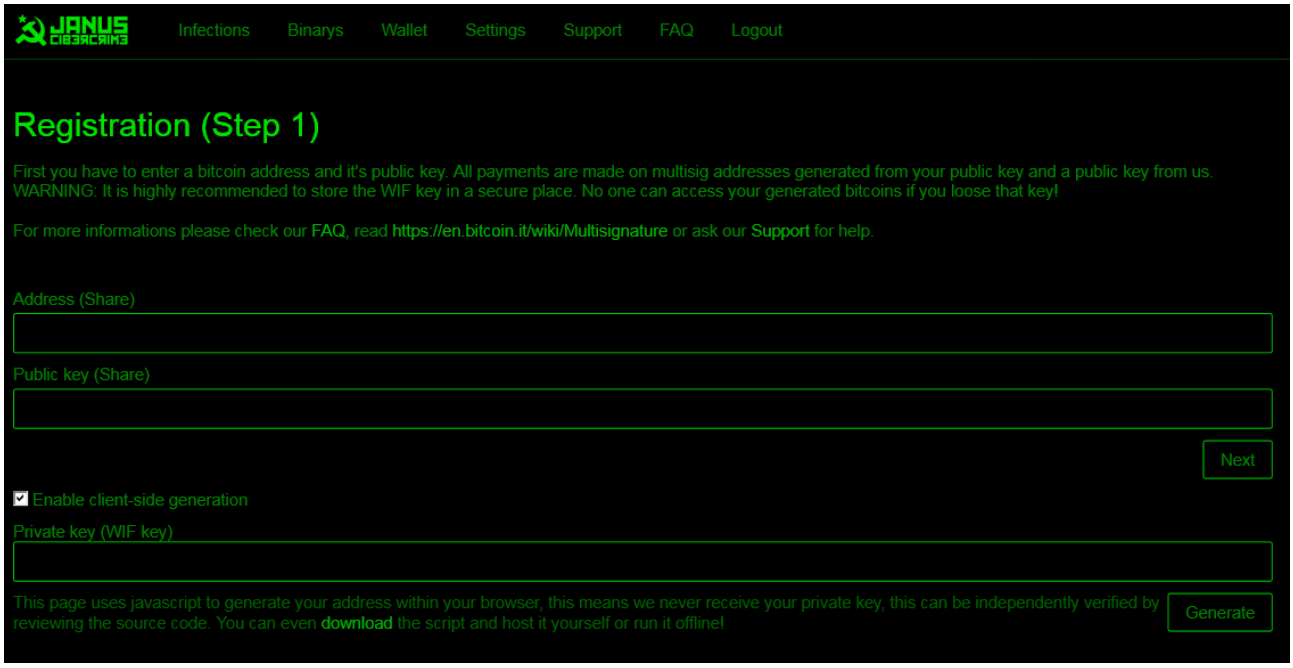
Программы-вымогатели все чаще сдаются в аренду на криминальном рынке

Рост популярности RaaS

Модель «Вымогатель как услуга» (Ransomware-as-a-Service, RaaS) — это не новое явление, но в 2016 году эта схема распространения программ-вымогателей продолжала совершенствоваться, и все больше вирусописателей предлагали свой вредоносный продукт «по требованию». Такой подход оказался чрезвычайно популярным среди злоумышленников, которым не хватает специальных навыков, ресурсов или желания создавать собственное вредоносное ПО.

Характерными примерами программ-вымогателей, появившихся в 2016 году и использующих эту модель, являются троянцы Petya/Mischa и Shark, который после «ребрендинга» получил имя Atom.

Эта бизнес-модель постоянно развивается и усложняется:



Партнерский сайт программы-вымогателя Petya

Для партнеров часто действует стандартная схема, основанная на комиссионном вознаграждении. Например, из «таблицы выплат» за распространение троянца Petya видно, что если продажи партнера составляют 125 биткойнов в неделю, то его недельный заработок составит 106,25 биткойнов.

Volume/Week	Share
<5 BTC	25%
<25 BTC	50%
<125 BTC	75%
>=125 BTC	85%

Таблица выплат за распространение троянца Petya

Существует также первоначальный взнос за использование программ-вымогателей. Например, тому, кто хочет воспользоваться шифровальщиком Stompado, нужно заплатить всего $39.

Учитывая, что другие киберпреступники предлагают услуги в области распространения спама, создания требований о выкупе и т.д., начинающему злоумышленнику достаточно легко вступить в игру.

От партнерских сетей с комиссионным вознаграждением до клиентской поддержки и брендинга

Преступники предлагают клиентскую поддержку, чтобы обеспечить максимальный процент оплаты выкупа жертвами

Наиболее «профессиональные» киберпреступники предлагали своим жертвам консультационную и техническую поддержку, помогая им приобрести биткойны для уплаты выкупа, а иногда даже вступали в переговоры с ними. При этом каждый их шаг подталкивал жертву к тому, чтобы заплатить выкуп.

Кроме того, специалисты «Лаборатории Касперского», изучая программы-вымогатели в Бразилии, заметили, что во многих атаках достаточно большое значение придавалось брендингу. Те, кто стремился привлечь внимание средств массовой информации и напугать клиентов, активно использовали резонансные события, имена известных людей или рекламные приёмы. Те же, кто предпочитал оставаться незамеченными, отказывались от искушения прославиться и оставляли своих жертв один на один с адресами электронной почты для связи со злоумышленниками и реквизитами для внесения биткойнов.

Биткойны по-прежнему в чести

В течение всего 2016 года наиболее популярные семейства программ-шифровальщиков по-прежнему требовали оплату в биткойнах. В основном суммы выкупа были умеренными, в среднем около $300, но некоторые киберпреступники требовали (и получали!) гораздо больше.

Другие группировки, в основном те, чьи кампании имели региональную направленность или управлялись в ручном режиме, зачастую предпочитали локальные варианты оплаты, хотя это лишало их возможности растворяться в толпе себе подобных, смешавшись с остальными группировками, использующими программы-вымогатели.

БИЗНЕС НА ПРИЦЕЛЕ У ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Программы-вымогатели атакуют компании каждые 40 секунд

В первом квартале 2016 года 17% атак с применением программ-вымогателей были направлены против корпоративного сектора — другими словами, в среднем во всем мире проводилось по одной атаке на ту или иную компанию каждые две минуты*. К концу третьего квартала эта доля выросла до 23,9% — в среднем одной атаки каждые 40 секунд.

По данным исследования «Лаборатории Касперского», в 2016 году каждая пятая компания по всему миру столкнулась как минимум с одним инцидентом IT-безопасности в результате атак с применением программы-вымогателя.

- 42% предприятий малого и среднего бизнеса испытали на себе атаки с применением программ-вымогателей за последние 12 месяцев.
- 32% атакованных компаний заплатили выкуп.
- Каждая пятая компания не сумела восстановить свои файлы даже после оплаты.
- 67% жертв программ-вымогателей полностью или частично потеряли свои корпоративные данные, причем у каждой четвертой жертвы на попытки восстановления доступа к данным ушло несколько недель.

* Оценка основана на следующем расчете: 17% от 372 602 уникальных пользователей, атаки программ-вымогателей на которых были заблокированы продуктами «Лаборатории Касперского» в течение первого квартала 2016 года, и 23,9% от 821 865 уникальных пользователей, атаки программ-вымогателей на которых были заблокированы продуктами «Лаборатории Касперского» в течение третьего квартала 2016 года

Каждой пятой компании малого и среднего бизнеса не удается вернуть свои данные даже после оплаты выкупа

Отраслей, мало подверженных риску, больше не осталось

Ключевыми факторами уязвимости компаний остаются социальная инженерия и человеческий фактор. Каждый пятый случай потери важных данных при атаках программ-вымогателей стал результатом неосторожности или неосведомленности сотрудников.

Некоторые отрасли страдают сильнее, чем другие, однако наши исследования показывают, что в зоне риска находятся все.

	Отрасль	% организаций, атакованных программами-вымогателями
1	Образование	23
2	Информационные технологии/ телекоммуникации	22
3	Развлечения/СМИ	21
4	Финансы	21
5	Строительство	19
6	Правительство/государственный сектор/ оборона	18
7	Производство	18
8	Транспорт	17
9	Здравоохранение	16
10	Розничная/оптовая торговля/досуг	16

«Мы обнаруживаем все больше целевых атак с применением программ-вымогателей: киберпреступные группировки тщательно отбирают жертв и атакуют их целевыми фишинговыми рассылками, ориентируясь на то, какие данные у них есть и/или насколько сильно они зависят от доступности этих ценных данных».

Джон Фоккер, Координатор группы по борьбе с киберпреступлениями, Национальное управление Нидерландов по противодействию преступлениям в области высоких технологий

Наиболее значительные атаки программ-вымогателей в 2016 году

- **Больницы стали популярными мишенями.** В результате операции отменялись, пациентов переводили в другие больницы и т.д., но последствия могли быть гораздо более серьезными.
  - Наиболее резонансная атака с использованием программ-вымогателей произошла в марте. Преступники заблокировали компьютеры медицинского центра Hollywood Presbyterian в Лос-Анжелесе и разблокировали их только после того, как получили выкуп в сумме $17 000.
  - Через несколько недель после этого инцидента атакам подверглись несколько больниц в Германии.
  - 28 учреждений национальной службы здравоохранения Великобритании сообщили о том, что стали жертвами атак в 2016 году.
- В сентябре **хостинг-провайдер виртуальных рабочих столов и облачных сервисов VESK** выплатил почти $23 000 в качестве выкупа, чтобы вернуть доступ к одной из своих систем
- В марте 2016 года **ведущие СМИ**, в том числе New York Times, BBC и AOL, подверглись атакам с использованием программ-вымогателей.
- Крупнейший исследовательский центр — **Университет города Калгари в Канаде** — признал, что заплатил около $16 000 за восстановление электронных писем, которые были зашифрованы и оставались недоступными в течение недели.
- **Небольшой полицейский участок в штате Массачусетс** вынужден был выплатить $500 выкупа (в биткойнах) за то, чтобы вернуть важные данные по расследуемым делам. Данные были зашифрованы программой-вымогателем после того, как один из сотрудников открыл вредоносное вложение в почте.
- **Под ударом оказался даже автоспорт**: в апреле одна из ведущих гоночных команд NASCAR рассталась с данными, стоимость которых оценивается в несколько миллионов долларов, после атаки программы-вымогателя TeslaCrypt.

ОТПОР ВЫМОГАТЕЛЯМ

Через применение технологий

Новейшие версии продуктов «Лаборатории Касперского» для небольших компаний были усилены функционалом для противодействия вредоносным программам-шифровальщикам. Кроме того, была выпущена новая бесплатная утилита для борьбы с программами-вымогателями, которую может загрузить и применить любая компания, независимо от того, какое защитное решение она использует.

Доступна новая бесплатная утилита для защиты от программ-вымогателей, совместимая с любыми антивирусными решениями

Утилита Kaspersky Anti-Ransomware Tool for Business — это «легкое» решение, которое может функционировать параллельно с другим антивирусным ПО. Утилита использует два компонента, необходимых для раннего обнаружения троянских программ, а именно распределенную облачную сеть Kaspersky Security Network и модуль Мониторинг активности, который отслеживает активность приложений.

Kaspersky Security Network быстро проверяет репутацию файлов и URL-адресов по облачной базе, а Мониторинг активности отслеживает поведение программ и обеспечивает проактивную защиту от не известных на данный момент версий троянцев. Особенно важно, что утилита может создавать резервные копии файлов, открываемых подозрительными приложениями, и осуществлять откат изменений, если действия программ будут признаны вредоносными.

Через сотрудничество: инициатива «No More Ransom»

На сегодняшний день в рамках проекта «No More Ransom» свыше 4400 пользователей смогли восстановить свои данные, а киберпреступники недополучили выкуп на сумму 1,5 миллиона долларов

25 июля 2016 года Национальная полиция Нидерландов, Европол и компании Intel Security и «Лаборатория Касперского» объявили о запуске инициативы «No More Ransom». Это некоммерческий проект, объединяющий государственные и частные организации с целью информировать людей об опасности программ-вымогателей и помогать им в восстановлении заблокированных данных.

В настоящее время на интернет-портале доступны восемь утилит для дешифровки файлов, пять из которых созданы «Лабораторией Касперского». Они позволяют восстанавливать файлы, зашифрованные более чем двадцатью типами вредоносных программ-шифровальщиков. На сегодняшний день свыше 4400 пользователей сумели восстановить свои данные, сэкономив более 1,5 миллиона долларов в результате отказа от выплаты выкупа.

В октябре к проекту присоединились правоохранительные органы еще 13 стран, включая Боснию и Герцеговину, Болгарию, Колумбию, Францию, Венгрию, Ирландию, Италию, Латвию, Литву, Португалию, Испанию, Швейцарию и Великобританию.

Евроюст и Европейская комиссия также поддерживают цели и задачи проекта. Ожидается, что в ближайшее время будет объявлено о присоединении к проекту новых партнеров — частных организаций и правоохранительных органов разных стран.

«Государственно-частное партнерство — это суть и сила инициативы «No More Ransom». Оно имеет принципиальное значение для эффективного и действенного решения проблемы, обеспечивая значительно более широкие возможности и охват, чем если бы правоохранительные органы действовали в одиночку».

Стивен Уилсон,
глава Европейского центра по борьбе
с киберпреступностью Европола

Как дать отпор вымогателям и обеспечить свою безопасность

1. Регулярно создавайте резервные копии данных.
2. Используйте надежное защитное решение. Следите за тем, чтобы основные его функции, такие как Мониторинг активности, были всегда включены.
3. Вовремя обновляйте ПО на всех своих устройствах.
4. Будьте осторожны с почтовыми вложениями и письмами от незнакомых людей. Если сомневаетесь, не открывайте их.
5. Если вы представляете компанию, вам необходимо также обучать ваших сотрудников и IT-специалистов. Храните конфиденциальную информацию отдельно от остальных данных, ограничивайте доступ к ней. Кроме того, у вас всегда должны быть резервные копии всех ваших данных.
6. Если вам не повезло и вы стали жертвой программы-шифровальщика, не паникуйте. Зайдите на наш сайт No More Ransom с незараженного компьютера — не исключено, что там найдется утилита, которая позволит вам расшифровать ваши данные.
7. И наконец, не забывайте, что применение вредоносных программ-вымогателей — это уголовное преступление. Обязательно заявляйте о таких случаях в правоохранительные органы.

**«Мы убедительно просим пользователей сообщать об атаках: каждый из потерпевших обладает важными уликами, которые могут серьезно помочь нам анализе проблемы. Мы, со своей стороны, готовы информировать этих пользователей о положении дел и защищать их от сомнительных сторонних «предложений» о расшифровке данных.
В то же время нужно повышать осведомленность правоохранительных органов и их готовность бороться с киберпреступлениями».**

Тон Маас, Координатор группы по борьбе с киберпреступлениями, Национальное управление Нидерландов по противодействию преступлениям в области высоких технологий

Почему не следует платить выкуп — рекомендации Национального управления Нидерландов по противодействию преступлениям в области высоких технологий

1. Заплатив, вы станете более привлекательной жертвой для киберпреступников.
2. Нельзя доверять киберпреступникам — нет никаких гарантий, что вы сможете восстановить свои данные, даже если заплатите выкуп.
3. В следующий раз размер выкупа для вас будет выше.
4. Платить — значит поощрять киберпреступников.

ВОЗМОЖНО ЛИ ПОБЕДИТЬ В БОРЬБЕ С ПРОГРАММАМИ-ВЫМОГАТЕЛЯМИ?

Да, мы считаем, что это возможно, но только объединив усилия. Программы-вымогатели — это прибыльный криминальный бизнес. Чтобы остановить его, нам всем необходимо объединиться, разрушить сложившиеся криминальные схемы и сделать так, чтобы киберпреступникам было все труднее проводить свои атаки и получать от них прибыль.

Securelist

Ресурс экспертов «Лаборатории Касперского» с актуальной информацией о киберугрозах

Сайт «Лаборатории Касперского»

Блог Евгения Касперского

B2C блог «Лаборатории Касперского»

B2B блог «Лаборатории Касперского»

Новостная служба «Лаборатории Касперского»

Блог Kaspersky Academy