Вымогательские программы и методы противодействия их активности

05/05/2017

Вымогательские программы неоднократно становились информационным поводом для изданий, специализирующихся на сфере IT. Они оставляют пользователей без результатов многомесячной работы или личных фотографий и наносят огромный ущерб компаниям, парализуя их деятельность. Редакция SecureNews предложила экспертам поделиться своими мнениями об этой угрозе и рассказать о методах борьбы с ней.

Прежде всего мы представили на суд специалистов следующий тезис: «Вымогательские программы являются наибольшей угрозой для данных пользователей и компаний». Согласны ли с этим эксперты?

Елена Стрелкова, менеджер по маркетингу **Trend Micro Россия**:

«Программы-вымогатели действительно являются сегодня одной из самых серьезных угроз как для обычных пользователей, так и для компаний по всему миру. Только за прошедший год число семейств программ-вымогателей выросло на 752%, а убытки организаций от этого вида угроз достигли 1 миллиард долларов США. В 2017 году, по нашим прогнозам, рост количества новых семейств программ-вымогателей несколько замедлится и достигнет порядка 25%. Это связано, в том числе, с появлением сервиса «программа-вымогатель-как услуга». Его идея заключается в том, что киберпреступники готовы по заказу создавать новые уникальные виды программ-вымогателей. В результате, у злоумышленников появляется возможность выбирать жертву (компанию или рядового пользователя) более целенаправленно, чтобы получить максимум финансовой выгоды. Однако, несмотря на замедление темпов роста числа таких программ, мы прогнозируем, что их воздействие в этом году будет распространяться на новые устройства, например, PoS-терминалы, банкоматы и устройства Интернета вещей».

Эксперт Центра информационной безопасности компании **«Инфосистемы Джет» Павел Волчков** считает, что степень угрозы, исходящей от вымогательских программ, отличается в зависимости от жертв их активности:

«Если говорить о предприятиях малого бизнеса, то, безусловно, для них программы-вымогатели (и не только программы, но и вообще деструктивные действия, направленные на нарушение целостности данных и доступности ИТ-сервисов) представляют наибольшую угрозу. Для малого бизнеса, не заботящегося о бэкапах, порой единственным выходом при встрече с программой-вымогателем является выполнение требований злоумышленника. При этом, как ни удивительно, авторы вредоносных программ зачастую дорожат своей репутацией и реально расшифровывают файлы, чтобы новые жертвы, ищущие в интернете информацию о вирусе, находили отзывы только «довольных» пострадавших». Вероятность восстановления данных высока.

Если же вы столкнулись с ситуацией, когда злоумышленник проник в сеть, удалил какие-то данные и просит деньги за их восстановление, вероятность их восстановления значительно ниже, так как анонимный злоумышленник никак не заинтересован в возвращении вам данных. Одним из вариантов проверки может быть запрос объемов исходящего трафика у интернет-провайдера. Если в момент компрометации значительные объемы данных не передавались из

сети, значит, злоумышленник не скачивал ваши данные и, следовательно, ничего возвращать не будет.

Говоря о среднем и крупном бизнесе – программы-вымогатели, конечно, представляют угрозу и здесь, но не столь существенную в сравнении с другими типами атак.

С точки зрения обычного человека – программы-вымогатели вряд ли являются большой угрозой. Да, потеря личной информации (например, архива фотографий) вследствие работы шифровальщика – крайне неприятное событие. Но все же, по моему мнению, атаки, направленные на хищение средств физических лиц в системах ДБО (дистанционное банковское обслуживание), представляют большую угрозу».

Также мы попросили экспертов дать свою оценку активности вымогательского ПО в 2016 и 2017 году: имеет ли место тенденция к ее росту?

Виктория Носова, консультант по безопасности **Check Point Software Technologies:**

«Активность вымогательского ПО (ransomware) находится на рекордно высоком уровне. В соответствии с ежемесячным отчетом Threat Index, который компания Check Point Software Technologies готовит на основе данных о десятках тысяч актуальных атак по всему миру, в сентябре прошлого года вымогательское ПО Locky впервые вошло в тройку самых опасных и популярных вредоносных программ в мире. В марте 2017 года в тройку самых активных программ-вымогателей вошел шифратор Cryptowall.

К сожалению, сегодня нет предпосылок для того, чтобы этот опасный тренд начал терять актуальность. Скорее наоборот: рост активности вымогательского ПО — одно из самых уверенных предсказаний на 2017 год. Так, наряду с Locky в 2016 году в поле зрения ИБ-экспертов чаще всего попадало вредоносное семейство Cerber. В августе 2016 года Check Point опубликовал отчет, который описывал работу Cerber — Ransomware-as-a Service. Каждый день в среднем запускаются 8 новых кампаний Cerber, а ежегодный прогнозируемый доход этой франшизы — 2,3 миллиона долларов США.

Причина такой популярности этого вида вредоносных программ в том, что очень часто жертвы идут на требования хакеров и платят выкуп. В результате хакеры видят прибыльность и эффективность этого вектора атаки».

Яков Гродзенский, руководитель направления информационной безопасности компании **«Системный софт»**:

«Тенденция к росту ущерба от вымогательского ПО наблюдается в последние 3-4 года, и пока нет никаких объективных причин прогнозировать ее изменение. Активность вымогателей растет в геометрической прогрессии, потенциальный ущерб от нее уже стремится к цифре миллиард долларов в год, поэтому в 2017 году этот тренд сохранится».

Алексей Королюк, генеральный директор хостинг-провайдера **REG.RU**:

«Безусловно, тенденция к росту есть, так как это направление имеет большие перспективы на дальнейшее развитие и предполагает большие доходы для киберпреступника. Как следствие, количество атак, направленных против компаний, будет только расти, поскольку хранящаяся у них информация более ценна по сравнению с той, что имеется у частных лиц. Автоматизированные атаки с применением программ-вымогателей также позволят обогатиться за счет одновременного обмана множества жертв, каждая из которых предоставляет небольшую сумму. Чаще всего атакам будут подвергаться устройства IoT (интернет вещей)».

Самый важный вопрос, который волнует пользователей: «Как можно противодействовать активности таких программ?» Мы попросили экспертов рассказать о методах борьбы с вымогательским ПО.

Алексей Качалин, заместитель директора по развитию бизнеса в России компании **Positive Technologies**:

«Пользователи являются более частой целью вымогателей по сравнению с корпорациями, но по объему выплачиваемых средств компании значительно опережают, а, следовательно, более интересны для злоумышленников. Следует ожидать популяризации ставшего классическим механизма: точечная атака новыми инструментами на ценную мишень, далее – серия атак на цели поменьше и массовый запуск нового «инструмента». Чем активней компании будут заниматься безопасностью и расследованием инцидентов, тем больше шансов у пользователей успеть подготовиться (обновить средства защиты) и предотвратить заражение. Это значит, что необходимо применять современные средства мониторинга событий и расследования инцидентов (SIEM), системы обнаружения атак на основе машинного обучения (WAF), а также уделить внимание повышению осведомленности персонала в области информационной безопасности.

В отличии от бизнес-среды, пользователям мобильных устройств рекомендуется уделять повышенное внимание безопасности приложений — в частности, скачивать их только из официальных магазинов, и даже в случае с легитимными приложениями использовать настройки для ограничения прав доступа к персональным данным и потенциально опасным действиям. Актуальными остаются все советы по безопасности авторизации, включая двухфакторную аутентификацию и сложные пароли. Использование сервисов на основе систем спутникового позиционирования желательно дублировать альтернативными методами навигации».

Антон Карданов, руководитель сектора ИБ компании AT Consulting:

«Основной способ противодействия — это использование антивируса и воздержание от посещений и тем более действий (скачивание информации, переход по ссылкам) на подозрительных сайтах и в электронных сообщениях, пришедших от непроверенных отправителей.

Если вы все-таки стали жертвой вымогательского ПО, то настоятельно рекомендуется не платить деньги и не верить угрозам о привлечении к ответственности в соответствии с законодательством.

Единой последовательности действий при блокировке нет, поскольку таких программ много и конкретные меры по борьбе с ними несколько отличаются. Но если сообщение о блокировке появилось на сайте, постарайтесь закрыть браузер (в том числе через принудительное закрытие или диспетчер процессов), не переходя ни по каким ссылкам, приведенным в окне блокировки.

Так же для конкретного случая способ борьбы можно найти в интернете, описав характер ситуации и текст сообщения, выдаваемого вымогательским ПО (опять же, используя информацию с сайтов, которые вызывают доверие).

Что касается отличия методов противодействия для организаций и для рядовых пользователей, то отличия существенного нет, так как техника реализации угрозы одна и та же. Главное отличие состоит в том, что рядовой пользователь в большинстве случаев рискует только своими данными, а тот же корпоративный пользователь ставит под угрозу деятельность компании. Донести это до пользователя как раз и является одной из задач службы информационной безопасности организации».

Яков Гродзенский:

«Все методы защиты от вымогательского ПО известны. Это использование бэкапов, внедрение программ повышения осведомленности о фишинге для сотрудников организаций, внедрение специализированных «песочниц», через которые будет пропускаться подозрительные файлы, причем как на периметре сети, так и на рабочих станциях пользователей, а также сканирование компьютеров на уязвимости и ограничение запуска приложений на компьютерах пользователей. Все вышеперечисленные методы характерны для корпоративного сектора, говоря же о рядовых пользователях, то я бы все-таки посоветовал регулярно пользоваться бэкапированием компьютеров и особенно тщательно относиться к тем письмам, которых вы не ждали, обращая внимание, не только, но в том числе, и на адрес отправителя».