КИБЕРУГРОЗЫ СЕГОДНЯ: предупрежден – значит, вооружен

Н.Гребенников, вице-президент по разработке компании Acronis

УДК 004.056.53, DOI: 10.22184/2070-8963.2017.65.4.76.78

В статье представлен сводный анализ киберугроз в 2016 году и прогноз на 2017 год. Что нужно знать, чего опасаться и к чему готовиться?

Главные киберугрозы 2016 года

Во-первых, программы-вымогатели продемонстрировали не только количественный, но и качественный рост в 2016 году. По статистике компании McAfee, число новых экземпляров программ-вымогателей составило около 4 млн (увеличение – на 80% экземпляров с начала года), а по данным "Лаборатории Касперского" – до 7,2 млн. При этом вымогатели начали использовать новые технологии для атак, в том числе частичное или полное шифрование дисков, шифрование веб-сайтов, использование доверенных приложений для обмана средств защиты и более сложные эксплоиты. Аналитики большинства компаний в области компьютерной безопасности сходятся во мнении, что 2016 год можно назвать годом программ-вымогателей, которые закрепили за собой звание главной киберугрозы.

Во-вторых, зафиксирован огромный рост вредоносных программ для мобильных устройств. Данная тенденция была предсказана еще в 2014 году, однако именно в прошлом году общее количество уникальных экземпляров вредоносных приложений для Android достигло устрашающей цифры в 19,2 млн (в 2015 году – "лишь" 10,7 млн). По данным компании Trend Micro, в 2016 году значительно выросло количество программ-вымогателей для мобильных устройств, что объединяет первый и второй тренды. Так, в четвертом квартале было обнаружено в три раза больше экземпляров вредоносного ПО по сравнению с тем же периодом 2015 года. Все эти программы-вымогатели имеют общий принцип воздействия на пользователя: оскорбление, травля, запугивание, вымогательство. Основную долю составили: блокировщики экрана, которые нарушали работу Android; маскировщики под обновления системы и популярных игр. Также доверчивые пользователи, сами того не понимая, предоставляли программам-вымогателям доступ к системе, где они могли изменить пароль для блокировки экрана устройства.

В-третьих, про угрозы для Интернета вещей говорится уже давно, но именно в 2016 году появились первые прототипы атак на IoT. Например, это ботнет Mirai, сканирующий Интернет в поисках уязвимых устройств. При этом на каждое устройство производится атака на подбор пароля с использованием базы из 60 паролей по умолчанию. Таким образом было заражено множество камер наружного наблюдения и других устройств, что позволило осуществить атаку на инфраструктуру целой страны.

При этом обычные пользователи признают самыми страшными на данный момент пять видов киберугроз: трояны-вымогатели, шифрующие файлы на Windows (они становятся все изощреннее и используют крайне продвинутые способы распространения); трояны-вымогатели,

блокирующие Android-устройства (бум такого рода угроз наблюдался в 2016 году и будет нарастать в 2017-м); трояны-вымогатели, блокирующие работу компьютера через заражение главной загрузочной записи жесткого диска (MBR); компрометация баз пользователей публичных сервисов типа Twitter, LinkedIn, Dropbox и Vkонтакте; перехват разговоров и кража денег со счета через уязвимости протокола SS7/OKC7 (защититься от нее никак нельзя, а атака не требует ни специального дорогостоящего оборудования, ни специальных знаний).

Прогнозы главных киберугроз на 2017 год

Программы-вымогатели останутся основной угрозой для пользователей и будут расширять поверхность атаки. Преступники могут заработать до 5 млрд долл. США в 2017 году, получая выкуп от своих жертв. Вследствие взрывного роста этой формы высокотехнологичного воровства многие пользователи и компании стали все чаще защищать свои данные от программ-вымогателей с помощью облачных хранилищ и сервисов резервного копирования. Однако количество новых экземпляров и модификаций вымогателей будет расти, они станут более скрытными и с помощью автоматизации смогут атаковать облачные системы, медицинские устройства: стимуляторы сердечной деятельности, МРТ, а также стратегически важную инфраструктуру и серверы. Киберпреступникам несложно будет получать выкуп от организаций, так как они более склонны поддаваться вымогательству для сокрытия фактов успешной атаки.

Следующим этапом развития вымогателей станет эра "червей-вымогателей" – вредоносных программ, которые не только шифруют файлы, но и активно распространяются внутри организации или междомовой сети.

Продолжится распространение готовых инструментов для кибератак и более разрушительных атак на отказ в обслуживании. Будет набирать еще большую популярность бизнес-модель "вымогательское ПО как услуга" – удобство использования и низкая стоимость модели привлечет в отрасль очень много новичков.

На первый план выходит безопасность облачных сервисов. Финансовые учреждения не спешат использовать облачные технологии, но рано или поздно большинство из них не смогут игнорировать преимущества использования подобных технологий, поэтому проблема безопасности облачных решений встанет еще острее. Организациям следует сфокусироваться на безопасности не только устройств, но и пользователей и информации во всех приложениях, а также на услугах для защиты от программ-вымогателей и других атак. "Облачная безопасность как услуга" позволит сократить расходы на приобретение и обслуживание средств защиты, в частности межсетевых экранов.

Такие сайты, как WikiLeaks продолжат обнародовать секретные политические документы. Коммуникационный протокол SS7, созданный в 70-х годах прошлого века и являющийся основой современной сотовой связи, имеет множество уязвимостей и содержит лишь базовые механизмы безопасности. Это позволяет злоумышленникам, находящимся, например, в Аргентине, перехватить звонки в США или Китае без каких-либо сверхдорогих компьютеров и ПО.

Интернет вещей продолжит представлять собой растущую угрозу. Только в прошлом году насчитывалось около 6,4 млрд подключенных устройств по всему миру. Эта цифра, по прогнозам компании Symantec, возрастет до 20,6 млрд к 2020 году, и количество уязвимостей по мере

развития технологии Интернета вещей будет только возрастать.

Современные автомобили могут содержать до 100 млн строк программного кода, становятся более умными, автоматизированными, и, самое главное, большинство из них подключены к интернету. Но многие водители не подозревают, какое ПО находится в их автомобиле. Использование свободно распространяемого ПО в автомобиле может привести к масштабным хакерским атакам, таким как удержание автомобиля для вымогательства, взлом системы самоуправляемых автомобилей с целью определения их местоположения для угона, несанкционированное наблюдение и сбор данных и др.

Люди всегда были и остаются самым слабым звеном любой системы защиты. Сотрудники компаний нарушают правила безопасности организаций, поэтому начнет набирать популярность сервис страхования от кибератак. Решение Google начать отмечать сайты без шифрования (протокол http вместо https) как небезопасные, с одной стороны, позволит предотвращать атаки с подменой адресов, с другой – такой подход может значительно снизить работу по стандартам безопасности в долгосрочной перспективе.

Глобальные институты – города и целые страны – адаптируют свою политику к аспектам кибербезопасности. По прогнозам IDC, к 2020 году 80% государств будут иметь официальную политику кибербезопасности и, по крайней мере, у 30% будут введены должности на уровне кабинета министров, ориентированные исключительно на кибербезопасность; к 2020 году 45% правительств будут обращаться к новым технологиям, таким как DRM и blockchain для защиты данных.

Как защититься от программ-вымогателей

Компания Acronis провела собственное исследование того, как пользователи защищают свои данные от программ-вымогателей, которые становятся самой серьезной угрозой для данных в 21 веке. Опросив пользователей по всему миру, компания пришла к неутешительному выводу: большинство респондентов ничего не знают об опасностях и совершенно не готовы им противостоять. Более 62% участников опроса заявили, что никогда не слышали о программах-вымогателях; более 67% сообщили о высокой ценности их личных данных, документов, фотографий, видео и музыки, но только 5,8% из них осознают, что восстановление данных после атаки программ-вымогателей может стоить более 500 долл. США.

Между тем, согласно данным ФБР, только за прошедший год преступники получили от жертв программ-вымогателей более 1 млрд долл. И в то время, как основное внимание было приковано к широко известным случаям, связанным с больницами и различными правительственными организациями, атаки на домашние компьютеры почти не освещаются в прессе. Нарушения в сфере безопасности грозят не только предприятиям, но и обычным людям. Мы привыкли считать это проблемой бизнеса или правительства, но на самом деле большая часть программ-вымогателей атакует обычных пользователей – тех, у кого в принципе есть электронная почта и компьютер.

При этом дополнительные данные исследования свидетельствуют: в 51,8% семей есть более, чем четыре цифровых устройства; 26,6% считают безопасность наиболее важным элементом резервного копирования; значительная доля респондентов (10,5%) считает очень важными данные своего профиля в Facebook.

Атаки вредоносных программ и защита от них постоянно эволюционируют. Поскольку использование резервного копирования доказало свою надежность, как средство защиты от программ-вымогателей, преступники начали разрабатывать новые варианты вредоносных программ, которые находят и атакуют в том числе и резервные копии данных.

В любом случае пользователям рекомендуем всегда придерживаться четырех простых правил защиты данных:

- создавайте резервные копии важных данных; выбирайте ПО для резервного копирования с локальным и облачным хранилищем, а также с активной защитой от программ-вымогателей;
- регулярно обновляйте операционную систему и программное обеспечение, это не позволит киберпреступникам использовать известные уязвимости систем;
- будьте внимательны при получении подозрительных писем, ссылок и приложений: чаще всего киберпреступники проникают в ваши системы, когда вы открываете зараженное приложение к письму или переходите по ссылке на вредоносный сайт;
- установите антивирусное ПО на свой компьютер и включите его автоматическое обновление; если вы пользуетесь ПК, убедитесь, что ваш Windows Defender включен и обновлен. ■