профиль

31.05.2017 | Екатерина Буторина

Заурядный троянец

Как мир пытается побороть киберэпидемии

Россия инициирует в ООН международную конвенцию о сотрудничестве в противодействии киберпреступности, сообщил на прошлой неделе МИД РФ. Этот же вопрос станет одной из центральных тем и на нынешнем Петербургском международном экономическом форуме (ПМЭФ). Вкратце главные вопросы этой панели звучат так: как бороться с киберпреступностью, что делать? Ответ экспертов, впрочем, тоже поражает своей простотой: мойте руки перед едой, вернее, перед выходом в глобальное информационное пространство.

Конечно, хакеры изобретательны, теневой рынок их услуг расширяется, ущербы компаниям, госорганам, частным лицам исчисляются миллиардами, но чаще всего черви, троянцы и прочие вирусы проникают в киберорганизм компаний из-за банальной небрежности их сотрудников, если угодно, нарушения элементарных правил «информационной гигиены».

Плачь и раскошеливайся

Именно так и произошло в середине мая, когда одной из главных новостных тем стала пандемия вируса-вымогателя Wanna Cryptor (или WannaCry, «хочется плакать»), который блокировал компьютеры жертв, сообщая, что вся содержащаяся на них информация зашифрована, а за расшифровку надо заплатить $300–500. «Всего за сутки вирус-шифровальщик атаковал 200 000 компьютеров в 150 странах мира, – рассказали в компании по борьбе с киберугрозами Group-IB. – Вирус прошелся по сетям университетов и школ в Китае, заводов Renault во Франции, телекоммуникационной компании Telefonica в Испании и железнодорожного оператора Deutsche Bahn в Германии. Из-за заблокированных компьютеров в клиниках Великобритании пришлось отложить операции, а региональные подразделения МВД РФ не смогли выдавать водительские права». По некоторым данным, вирус поразил и компьютерную сеть Следственного комитета РФ, но официального подтверждения эта информация не нашла. Среди российских компаний в пострадавших числился «Мегафон».

WannaCry специализируется на компьютерах с оперативной системой Windows, отыскивая в них уязвимые места. Этот вирус – гибрид проверенной платформы для шифрования файлов жертв и вымогания денег за расшифровку с новым инструментом распространения, основанным на уязвимости в Windows, поясняет заместитель директора Центра информационной безопасности компании «Инфосистемы Джет» Андрей Янкин. «Данные об этой уязвимости были похищены у АНБ США и затем опубликованы неизвестными, именующими себя The Shadow Brokers», – говорит эксперт. Вектор распространения WannaCry исключительно прост, объясняет заместитель директора центра компетенции по экспертным сервисам Positive Technologies Алексей Новиков: «Программа не распространялась ни через письма, ни через фишинговые вложения, ни каким-либо иным способом. Ее запустили на одной или нескольких машинах, и дальше уже сама машина выбирала в произвольном порядке IP-адреса и искала открытый 445-й порт. Если он был открыт, происходила эксплуатация уязвимости, заражение машины и далее по цепочке». А руководитель российского исследовательского центра «Лаборатории Касперского» Юрий Наместников назвал вирус «заурядным троянцем»: «Наши защитные продукты детектируют его по нескольким вердиктам – Trojan–Ransom.Win32.Scatter.uf; Trojan–Ransom.Win32.Fury.fr; PDM: Trojan.Win32.Generic. Однако основная причина столь масштабной эпидемии – не сам троянец, а метод распространения при помощи недавно закрытой уязвимости в системах Windows.

Эпидемия WannaCry длилась двое суток, 12–14 мая. Но уже 13 мая программист из Великобритании, пользующийся аккаунтом @MalvareTechBlog в Twitter, смог случайно остановить вирус-вымогатель. Как пояснили в Российской ассоциации электронных коммуникаций (РАЭК), это произошло благодаря регистрации доменного имени, к которому обращалась программа, поражавшая компьютеры. «Программист зарегистрировал домен, чтобы проследить активность хакерской программы, – рассказали в ассоциации. – В итоге выяснилось, что адрес этот был зашит в коде вируса на случай необходимости его остановить. Атаку удалось остановить благодаря регистрации этого доменного имени, однако уже 14 мая появилась обновленная версия вируса, которая обходит это препятствие». По оценкам специалистов, более 1,3 млн компьютерных систем до сих пор уязвимы перед вирусом WannaCry.

Мойте руки перед едой

Об уязвимости собственной ОС в Microsoft знали за месяц до появления WannaCry, выпустили патч – программу-заплатку, закрывающую эту уязвимость. «Однако применить ее успели не все, – говорит Янкин. – Речь идет не о какой-то хитроумной атаке, а о банальной гигиене информационной безопасности (ИБ) – реальная защищенность многих компаний оставляет желать лучшего. Наши данные говорят о том, что число пострадавших в России весьма существенно. Где-то эпидемия вывела из строя отдельные машины, а где-то полностью блокировала работу бизнеса». По приведенной Новиковым аналогии компании не соблюли элементарного правила «мытья рук перед едой».

«Глядя на масштаб заражения, становится ясно, что «накатили» предложенные Microsoft обновления немногие, – констатирует эксперт. – И эта ситуация отнюдь не случайность и не исключение из общего правила – к обновлениям во многих организациях в принципе относятся наплевательски». В частности, в ходе работ по тестированию на проникновение эксперты Positive Technologies в 2016 году выявили уязвимости, связанные именно с отсутствием обновлений, в 87% случаев, и 67% из них имели высокую степень опасности. «Возраст известных уязвимостей, выявляющихся на проектах, порой исчисляется даже не месяцами, а годами», – добавляет Новиков.

Специалистов сложившаяся ситуация не удивила – если известно об уязвимости, значит, и охотники на нее найдутся. Однако по своему масштабу подобная эпидемия – явление нечастое. Последний раз такое случилось в 2008 году. «Червь Conficker заразил миллионы компьютеров похожей уязвимостью, – говорит Новиков. – Он не обладал деструктивными функциями, поэтому последствия были не такими серьезными. Но потенциал был уже тогда». Хотя патч на уязвимость, через которую проникал червь, выпустили тогда же, 10 лет назад, специалисты по ИБ до сих пор иногда встречают ее в сетях компаний, признает Янкин. «С учетом того, насколько разрослись ИТ-инфраструктуры за последнее время, WannaCry, на мой взгляд, недотягивает до легенд прошлого, таких как MyDoom, ILOVEYOU и того же Kido, – считает эксперт. – Последствия этих атак оцениваются в десятки миллиардов долларов. Думаю, после подсчета последствий атаки WannaCry таких высот не возьмет».

Заработки и ущербы

«Повторная эпидемия WannaCry теперь вряд ли возможна, – считает Наместников. – А вот точечные атаки с использованием тех же уязвимостей, что и в WannaCry, идут уже сейчас. Все киберзлодеи мира увидели, что инструменты, которые были опубликованы группировкой Shadowbrokers, очень эффективны, и, естественно, воспользуются моментом, чтобы получить доступ и закрепиться в уязвимых системах». Но так ли много награбили преступники? За разблокировку зараженных компьютеров злоумышленники требовали выкуп в размере $300–600, а за день заработали $42 тыс. «Мы знаем об этом доподлинно, ведь биткоин-кошельки устроены таким образом, что их содержимое (но не принадлежность) видно любому, – говорят в Group-IB. – Сумма для киберпреступного мира смехотворная, и она указывает на перелом в человеческом восприятии шифровальщиков как явления: люди больше не готовы платить за расшифровку, при 200 тыс. заражений заплатило всего 100–150 человек». Эксперты предполагают, что атака WannaCry таким образом «станет одновременно пиком и концом эпохи шифровальщиков».

«Заработок» распространителей WannaCry настолько низок, что, возможно, они не смогли даже окупить свои инвестиции в создание и распространение вредоносного ПО, считает Янкин. Но гораздо существенней сумма ущерба, понесенного пораженными вирусом компаниями и госструктурами. «Объем рынка киберпреступности оценивается в десятки миллиардов долларов в год, – говорит он. – Урон от киберкриминала оценивается на один-два порядка выше и измеряется в триллионах долларов. Весьма разрушительный бизнес. WannaCry не исключение. Злоумышленники нанесли урон, вероятно, на сотни миллионов долларов».

Только в период с 2012-го по 2015 год совокупный ущерб от деятельности киберкриминала составил $790 млн – эту оценку в «Лаборатории Касперского» сделали на основе анализа публичной информации об арестах подозреваемых в совершении финансовых киберпреступлений и собственных данных. «Из этой суммы около $280 млн было украдено преступниками в странах бывшего Советского Союза, – говорит Наместников. – Разумеется, эта цифра учитывает лишь подтвержденный ущерб, информация о котором была получена правоохранительными органами в ходе следственных мероприятий. В реальности киберпреступниками могли быть украдены значительно большие суммы».

Эпидемия вещей

А ведь WannaCry – лишь малая и далеко не значительная часть киберпреступного мира, который непрестанно эволюционирует. «Локеры, требующие выкуп за возвращение контроля за вашими бытовыми приборами, постепенно превратились в криптолокеров и локеров аккаунтов, а затем превратятся в локеров «умных» устройств», – приводит пример Новиков. Общее ухудшение экономической ситуации и, как следствие, снижение затрат на обеспечение безопасности увеличивает риски финансовых компаний, говорит эксперт, и предрекает уже в этом году рост в 30% атак на банки, процессинговые компании, брокерские компании, компании, занимающиеся денежными переводами. «Также для финансовой сферы будет характерно смещение цели атакующих с клиентов на сами банки», – говорит он. Отдельная тема – вредоносное ПО, которое атакует устройства интернета вещей. Это подключаемые к Сети чайники, камеры, роутеры, различные умные устройства и даже автомобили. «История больших эпидемий сейчас повторяется не для Windows, а уже для этих устройств (например, в ботнете hajime – созданной вредоносной программой сети – было около 300 000 зараженных девайсов), – объясняет Наместников. – Это происходит потому, что состояние безопасности этих вещей еще хуже, чем у компьютеров на заре 2000-х».

По-прежнему в тренде целевые атаки. «Особенную тревогу вызывает то, что преступники все чаще выбирают мишенью объекты критической инфраструктуры, например, нефтеперерабатывающие заводы и газопроводы, – говорит Наместников. – Продолжает активно развиваться сфера промышленного шпионажа и «конкурентной разведки», когда целью преступников становятся не деньги компании, а ценная информация, такая как контракты, деловая переписка». Смещение вектора преступной деятельности от массовых угроз к таргетированным атакам на корпорации и правительственные структуры эксперты видят по статистике: почти каждая четвертая компания (23%) в России считает, что уже становилась жертвой целевых атак.

«Жареный петух уже клюнул каждого»

На днях Group-IB сообщила о совместной операции специалистов по киберразведке компании и оперативников Управления «К» Бюро специальных технических мероприятий МВД РФ. Им удалось обнаружить и нейтрализовать кибергруппировку, «укравшую десятки миллионов рублей при помощи атак на мобильные устройства клиентов российских банков». Преступники использовали вредоносную программу Cron для ОС Android, с помощью которой ежедневно заражали порядка 3,5 тыс. устройств. В ноябре прошлого года 16 подозреваемых участников группировки задерживали сразу в шести регионах страны.

Действия преступной группы, распространяющей вредоносные программы под названием Cron («Крон») для ОС Android, были зафиксированы системой киберразведки Group-IB весной 2015 года. «Трояны для телефонов и планшетов окончательно вытеснили трояны для компьютеров, – констатирует глава департамента киберразведки, сооснователь Group-IB Дмитрий Волков. – В 2016 году ущерб от инцидентов с Android-троянами у физических лиц составил более 348 млн рублей. Почему именно пользователи ОС Android стали основной мишенью, объясняется просто: почти 85% смартфонов в мире работает на платформе Android».

По оценке «Лаборатории Касперского», с 2012-го по 2015 год правоохранительными органами разных стран (включая США, Россию, Белоруссию, Украину и страны Евросоюза) было арестовано более 160 русскоговорящих киберпреступников, входивших в состав малых, средних и крупных преступных групп, которые занимались хищением денежных средств с помощью вредоносного ПО по всему миру. Но процесс расследования подобных преступлений очень трудоемкий, признает Новиков: «Интернет имеет трансграничный характер, и для расследования необходима кооперация большого количества стран. Причем часто это сопровождается бюрократической волокитой. Безусловно, уже сложились тенденции к повышению числа успешных расследований, но, к сожалению, статистика пока еще не в пользу правоохранительных органов».

Если раньше проблема информационной безопасности была головной болью только для узкого круга IT-специалистов, то теперь это стало не только неотъемлемой частью бизнеса каждой компании, но и важной составляющей государственной политики почти любой страны. «Жареный петух уже клюнул каждого, и не раз, и пресса теперь уделяет ИБ большое внимание, – говорит Янкин. – Эти риски начали понимать на уровне бизнеса, государства. Это огромное достижение, но авторами его являются в первую очередь преступники, наращивающие обороты, а не сами безопасники».

Объединение усилий на международном уровне – наиболее эффективный способ борьбы с киберпреступностью, подчеркивает Наместников из «Лаборатории Касперского»: «Нашими партнерами среди правоохранительных органов являются Интерпол, Европол, Национальное подразделение высокотехнологичных преступлений полиции Нидерландов, полиция Лондона, а также многочисленные центры CERT (Computer Emergency Response Teams) по всему миру. Совместные действия помогают бороться с киберпреступлениями, позволяют уничтожать используемые преступниками ботнеты, способствуют запуску новых программ и инициатив в области информационной безопасности».

Но при этом многие вопросы остаются неразрешенными. Например, что именно может считаться актом кибератаки на государство, можно ли признать таковой заражение вредоносным ПО госпиталя, приводит пример Наместников. «Существует обширный документ НАТО, в котором сделана попытка систематизировать эти вопросы, – так называемый «Таллинский мануал», – говорит эксперт. – США в настоящий момент рассматривают сценарии вплоть до физического военного ответа на кибератаки, организованные другими странами. Но основная сложность в этом вопросе – это атрибуция, достоверная идентификация источника и организатора атаки. Все это является предметом обсуждения на самом высоком уровне, и в текущей ситуации такой диалог крайне необходим».