"Упс, ваши файлы закодированы" (WannaCry - и вправду хочется заплакать)

"Пришла беда, откуда не ждали"

Вечером в пятницу 12 мая вирусы начали искать доступ к компьютерным системам самых разных учреждений, а разблокировать их хакеры обещали только за биткоины.

И в самом деле, очень хотелось плакать (WannaCry), глядя на то, как застыли в недоумении врачи в английской больнице скорой помощи, где из-за блокировки компьютеров даже срочные операции сделать было невозможно. Это уже не Робин-Гуд, который наказывает толстосумов. Компания Avast обнаружила 75 тысяч заражённых компьютеров в 99 странах.К утру 16 мая стало известно о том, что атаки зафиксированы уже в полутора сотнях стран. Атаки в основном были нацелены на РФ, Украину и Тайвань, сообщили в Avast.

Легко представить состояние докторов в английской больнице скорой помощи, которые включают компьютер и вместо истории болезни пациента получают сообщение: "Упс, ваши файлы закодированы. Если вы не переведёте оплату в течение трех дней, сумма удвоится. В противном случае позже ваши файлы будут удалены полностью". Для ясности сообщения были на разных языках - русском, английском, китайском, немецком, испанском.

Понятно, что первым делом во многих странах виноватыми сделали неких "российских хакеров". С одной стороны да, гордиться можно тем, что наши теперь "впереди планеты всей", с другой непонятно, почему от атаки, по мнению экспертов, сильнее всего пострадала Россия.

Вирусная атака вызвала перебои в работе Министерства внутренних дел РФ, у сотового оператора "МегаФон", нападение отражали в банковском секторе и в ОАО РЖД, МЧС.

> "Две команды центра кибербезопасности работали всю ночь, по всем системам всех дочерних наших банков, тем более нашего российского главного банка "Сбербанка России". Можем еще раз подтвердить, что все системы работали, работают и будут работать надежно, безо всяких сбоев. Вирус достаточно известный, но канал, по которому он распространялся, оказался новым. И, по нашему мнению, ряд российских компаний, организаций этот вирус получили через сетевые каналы", — сказал Станислав Кузнецов, заместитель председателя правления "Сбербанка России".

Вирус блокировал компьютеры, работающие под управлением ОС Windows. По словам официального представителя МВД РФ Ирины Волк, в МВД блокировали порядка тысячи заражённых компьютеров (менее одного процента от общего количества) и локализовали активность вируса. Утечки же служебной информации, которая хранится на серверах, в МВД удалось избежать благодаря тому, что они работают не под Windows.

Кто стоит за WannaCry

...пока точно неизвестно. Британские СМИ тут же поспешили объявить о "российском следе", а Эдвард Сноуден заявил, что к созданию этого вируса причастно американское АНБ.

Страшновато делается, когда узнаёшь, что хакеры взломали систему управления крупнейшего оператора железных дорог Германии. В Ганновере из строя вышли все диспетчерские системы управления.

В Испании вирус остановил машиностроительный завод. Аналогичные ЧП – во Франции, Японии. В Бразильском Сан-Пауло из строя выведена система регионального суда.

По одной из версий, описание этого вируса было среди документов, опубликованных WikiLeaks. Вирус просто немного подновили, исправили и пустили в Сеть. Подтверждения этому, правда, пока нет.

Успешные военные операции с использованием компьютерных вирусов уже не новость. Разработанный спецслужбами США и Израиля червь Stuxnet три года атаковал ядерные объекты Ирана и нарушил работу почти тысячи центрифуг для обогащения уранового топлива. Таким образом, ядерная программа Ирана была отброшена на несколько лет назад.

По словам Эдварда Сноудена лучшая защита от бесчинств вируса - это создать резервную копию своих данных, и хранить эту копию на съёмном диске или флэшке. А чтобы защититься - не нужно открывать ссылки, которые ведут неизвестно куда.

Распространение вируса WannaCry удалось остановить, но совершенно случайно: британский

программист нашел подсказку в структуре самого вируса. Но если создатели внесут малейшие изменения, атака продолжится с той же силой, а потому российские специалисты кибербезопасности круглосуточно в режиме готовности.

О том, насколько серьёзна ситуация можно судить по тому, что своё мнение об атаке высказали лидеры многих стран.

Сегодня, 15 мая, в Пекине Президент РФ Владимир Путин подчеркнул, что хотя кибератака 12 мая не нанесла существенного ущерба российским учреждениям, но ситуация вызывает тревогу.

> "Что касается источника этих угроз, то, по-моему, руководство Microsoft прямо об этом заявило, сказали о том, что первичным источником этого вируса являются спецслужбы Соединенных Штатов, Россия здесь совершенно не при чем. Мне странно слышать в этих условиях что-то другое", - сказал Путин.

Со специальным заявлением выступила и премьер-министр Великобритании Тереза Мэй:

> "Мы знаем о том, что ряд медучреждений сообщили о хакерском нападении. Эта атака не была направлена именно на NHS (Национальная система здравоохранения). Это часть международной хакерской атаки, затронувшей учреждения в разных странах. Мы не располагаем информацией о том, что информация о пациентах попала в чужие руки".

В Австралии тему распространения вируса комментировали на высшем уровне, власти Индии заявили, что держат руку на пульсе, Руководитель полицейской службы Евросоюза Europol Роб Уэйнрайт привёл последние данные: пострадали минимум 200 тысяч организаций, частных лиц и компаний, включая крупнейшие корпорации.

Организованная преступность всё больше "оцифровывается"

Казалось бы, атака отбита, жизнь плавно входит в свою колею. Но вопросы остались, и весьма серьёзные. И обо всём, связанном с этой атакой мы расспросили Алексея Фёдорова, управляющего директора компании Avast Software по России и СНГ.

– Алексей, большинство крупных компаний в России, которые подверглись атаке, говорят, что ущерб был незначительным, и что все успели вовремя отреагировать. А как обстоят дела на самом деле, не занижают ли кое-где ущерб ради сохранения репутации?

– Полагаю, что в большинстве крупных компаний имеются довольно профессиональные IT службы, которые хорошо знают требования по безопасности корпоративных компьютерных сетей и жёстко им следуют. В частности, своевременно обновляют программное обеспечение, в том числе, отвечающее за безопасность. Также они внимательно следят за соблюдением сотрудниками правил компьютерной безопасности.

В случае с атакой WannaCry проблемы возникли, прежде всего, у тех организаций, которые своевременно не скачали обновление Windows, закрывающее уязвимость, не следили за актуальностью антивирусного ПО. Думаю, что большинство компаний действительно успели быстро ликвидировать возникшие проблемы до того как они привели к заметному ущербу.

– Атака началась вечером в пятницу. Это случайность или продуманный шаг?

– Вполне возможно, что расчет был на это – атаковать в пятницу вечером, когда рабочий день заканчивается, впереди несколько выходных и шансы на то, что компании своевременно отреагируют на атаку гораздо ниже.

– Как Вы считаете, это и в самом деле американские вирусы или же разработка хакеров, которые никак не зависят ни от каких правительств?

– Эта атака носит глобальный характер, нападению подверглись компании более чем в 70 странах мира, хотя Россия пострадала больше. Считаю, что этот случай носит криминальный характер, и нацелен на массовое вымогательство денег. Киберпреступность такого уровня не имеет национальности.

– Можно ли спрогнозировать дальнейшую логику действий злоумышленников?

– После блокирования первой волны распространения вируса (после того, как британский специалист по компьютерной безопасности обнаружил способ остановить распространение зловреда, зарегистрировав домен с бессмысленным названием, отсылка к которому была зашита в коде вредоносной программы), злоумышленники переписали исходный код, чтобы обойти блокировку. Вполне можно ожидать продолжения попыток массовых атак на организации в ближайшее время.

Скорее всего, хакеры предусмотрели способы быстро восстанавливать активность вируса в случае его блокирования.

– Были ли задействованы в атаке чат-боты?

– Вполне возможно, что для этой или последующих попыток распространения зловреда будут использовать чат-боты. Сама по себе технология чат-ботов была создана для автоматизации взаимодействия с посетителями сайтов, клиентами, обеспечения первой линии поддержки клиентов на сайте. Многие мессенджеры, социальные сети, компании используют эту технологию. Но, как и любая технология, она может использоваться как во благо, так и во вред. С помощью чат-ботов злоумышленники могут рассылать спам, ссылки на вредоносные ресурсы, заражённые файлы, собирать информацию о паролях или деталях доступа к счетам клиентов. Аваст защищает не от самих чат-ботов, а от попыток злоумышленников использовать чат-боты для распространения вирусов и получения незаконного доступа в компьютеры и сети потенциальных жертв. Такие попытки будут блокироваться нашими продуктами.

– Можно ли сказать, что за хакерами стоит организованная преступность, они сами постепенно превращаются в мафию, или же пока это одиночки? А когда все "возьмутся за руки" - это будет совсем страшно, и противостоять им будет невозможно?

– Сращивание организованной преступности и хакеров уже фактически произошло, время одиночек в прошлом. Атаки такого уровня требуют вовлечения целой группы лиц, что обычно квалифицируется как преступный сговор. Преступные деньги и серьёзная техническая подготовка хакеров создают большую опасность для информации и работоспособности сетей в глобальном масштабе.

– Действительно ли хакеры воспользовались существующими брешами в ПО или же они просто хорошо продумали техническое обеспечение атаки?

– И то и другое.

– Можно ли защититься от таких атак, распознают ли антивирусы новые вредоносы, не могут ли они спутать их с плановым обновлением ПО?

– Большинство современных антивирусов используют механизмы эвристического анализа, который позволяет распознать и предотвратить даже еще неизвестный зловред. Используются виртуальные песочницы, в которые помещаются подозрительные файлы и ссылки до того как будут допущены в корпоративную сеть. Очень важно держать антивирусную программу в постоянно актуальном состоянии. Кроме того, необходимо устанавливать самые последние обновления Windows и других популярных программ, которые закрывают возможные уязвимости.

– Интересно, сколько смогли заработать на атаке хакеры, какой ущерб они причинили и кому выгоднее всего эта мощная атака - нападающим или производителям антивирусов? Или же за всем этим шумом вообще стоят политики, которым главное доказать свою правоту и подогнать ответ, мол, русские хакеры опять набезобразничали?

– Думаю, что хакеры рассчитывали на получение многомиллионного дохода (в долларах) от действия своего зловреда, потому что атака носила глобальный характер. Полагаю, что и вложения в организацию атаки были немаленькими (речь может идти о десятках и сотнях тысяч долларов). Такая атака выгодна, прежде всего, ее организаторам, если им удастся добиться массового распространения и последующей массовой уплаты выкупа.

Производители антивирусов разрабатывают средства защиты от компьютерных угроз, без которых мир бы уже давно потонул в хакерском беспределе.

Политики, как всегда, используют разные удобные для них поводы, чтобы попиариться и укрепить свой рейтинг. Часто под это подтягиваются разные факты и трактуются так, как выгодно политикам в данный конкретный момент.

Что касается дальнейшего развития событий, то организованная преступность всё более "оцифровывается" и чувствует вкус к деньгам, которые можно добыть с помощью хакеров. Это означает, что стоит ожидать роста киберпреступности в глобальном масштабе, новых попыток массовых атак с основной целью – кража информации и денег, незаконное обогащение.

P.S. К утру 16 мая стало известно, что атаки остановить полностью так и не удалось. Правда, они стали менее активными и массовыми, Кроме того, разработчики изменили вирус и теперь действует уже не одна, а две его модификации.