Ваня, Петя и другие - не страшнее гриппа

"Вирусная атака, равной которой ещё не было, захватила весь мир. Пострадали сотни предприятий в десятках стран, потеряны ценнейшие данные" – как это ни странно, но волны вирусов начали повторяться с такой регулярностью, что мы даже особо удивляться таким новостям перестали. Впрочем, здравомыслящий человек, даже далёкий от IT, удивляется отнюдь не масштабу атаки, а реальным результатам.

Судите сами. Мощнейшая атака вируса Wanna Cry коснулась всех стран мира. Вирус-шифровальщик пробежался по тысячам предприятий, зашифровал огромное количество данных, а получили неведомые вымогатели… биткоины, денежный эквивалент, который составил 32 тысячи долларов. Не маловато ли для всемирной напасти?

Последовавшие за Wanna Cry атаки вирусов Vanya и Petya шума тоже наделали немало. Ещё бы – среди пострадавших оказались уже стратегические объекты – Чернобыльская АЭС, к примеру. Десятки стран, тысячи предприятий. Однако опять же невысокий, по сравнению с масштабами атаки, выкуп, сравнительно немного предприятий, работа которых была серьёзно нарушена вирусами, позволяют предположить, что шума безобразники Ваня и Петя наделали куда больше, чем вреда.

Ещё один вопрос, возникающий даже у неспециалиста, обладающего хотя бы малейшей способностью мыслить логически: неужели при нынешних достижениях компаний, создающих противовирусные программы, крупные предприятия экономят на защите своих сетей? Взлом сетей промышленного предприятия, аэропорта, спецслужб грозит катастрофой любого масштаба от локального до регионального, а то и вселенского (взять хотя бы ту же "взломанную" ЧАЭС, ЧП на которой чревато последствиями как минимум для всей Евразии).

Все эти вопросы я задала специалисту в сфере компьютерной безопасности, сотруднику НАГа Дмитрию Богословскому. И оказалось, что сомнения мои вполне обоснованны, а масштабы вирусной угрозы на сегодня, мягко говоря, весьма преувеличены.

> – Сегодня взломщики-вымогатели банально используют уязвимости Microsoft, которые по тем или иным причинам ещё не закрыты, – уверен Дмитрий. – Там, где операционная система постоянно обновляется и поддерживается в нормальном состоянии, всё в полном порядке. К примеру, WannaCry-Petya используют уязвимость десятилетней давности в протоколе SMB ещё первой версии.

– А как же разговоры о том, что во время атаки пострадали "Газпром" или Сбербанк?

> – Я думаю, что наиболее важная информация и сервисы в таких организациях содержатся в локальных сетях без выхода в публичные сети или имеет строго ограниченные разрешения на доступ, зональное разделение локальных сетей по рискам и соответствующие правила на доступ и хождение трафика, поэтому и вирусам к особо секретным данным не подобраться. Есть хорошее профессиональное правило – то что не разрешено, запрещено, и оно безукоснительно соблюдается в крупных компаниях.
>
> Способы заражения (размножения?) у большинства вирусов одни и те же – через инфицированное вложение в подозрительном письме, через уязвимость в браузере, в операционной системе. Сам по себе компьютер заразиться не может, вредоносный код должен запуститься локально. Запустить его без злого умысла может секретарша или кто-то из начинающих сотрудников, открывший инфицированный файл в электронном письме, прорвавшееся через спам-фильтры или скомпрометированный сайт, использующий уязвимость браузера для локального запуска. Ну, а дальше всё зависит от того, как построена система безопасности в компании – чем фирма крупнее, тем сложнее и мощнее защита, тем дальше от критически важной информации и сервисов компании будет остановлен и обезврежен вирус.
>
> Сетевые экраны, которые защищают сети предприятий – уже не диковинка, не редкость, а стандарт де-факто, поскольку позволяют защитить операционную систему и сетевые сервисы от несанкционированных действий. У нас в НАГе подобное оборудование пользуется стабильно высоким спросом. К примеру, межсетевые экраны Cisco ASA 5512-X, ASA5515-X и подобное оборудование, имеющее встроенную систему обнаружения вторжений позволят предотвратить несанкционированные действия ещё на начальном этапе. Кстати, ни одна из компаний, которая выбрала надёжные сетевые фильтры, не пострадала.

Правоту Дмитрия подтверждают и свежие новости. Вскоре после атаки в биткоин-кошелёк вымогателей поступила сумма, эквивалентная 10 тысячам долларов США. Втрое меньше, чем сумели получить авторы Wanna Cry.

Вымогатели, напомним, требовали у пострадавших по 300 $, но даже заплатившие не получили

ключей от зашифрованных файлов. Вымогатели, между тем, начали требовать за расшифровку уже 100 биткоинов, или 250 тысяч $ за расшифровку данных. Почему так дорого? Да якобы потому, что ключ универсальный и с его помощью доступ к потерянной информации получат все пострадавшие.

На сей раз, хакеры ссылались уже не на засвеченный кошелёк, а на чат в Dark Net. Эксперты, впрочем, продолжают сомневаться в том, что пострадавшие получат ключ. Более того, специалисты уверены, что Petya.A и разработан был для уничтожения пользовательских данных.

Так что милостей от судьбы ждать не приходится. За Ваней и Петей могут заявиться Джонни и Майкл. И защититься от их "длинных рук" очень даже можно. Главное – не экономить на безопасности и не вскрывать подозрительные письма, какими бы соблазнительными темами они не привлекали.