Крепко ли вы спите?

ВЯЧЕСЛАВ МЕДВЕДЕВ, ВЕДУЩИЙ АНАЛИТИК ОТДЕЛА РАЗВИТИЯ КОМПАНИИ "ДОКТОР ВЕБ"

Проблема безопасности всегда была актуальной — для компаний, государства в целом, да и для отдельных пользователей. Проводятся семинары, выпускаются стандарты и приказы, принимаются дорожные карты… Количество сообщений о доходах злоумышленников вызывает зависть у простых работников, сравнивших свои зарплаты с расходами после очередного новогоднего подорожания.

Но в итоге все остается в общем-то без особых изменений. В подавляющем большинстве компаний на обычных компьютерах и важных серверах в качестве защиты стоит "просто" антивирус, отвечающий на все вызовы угроз безопасности, как последний герой. Чего вы хотели? Кризис.

А в это время темная сторона гибко реагирует на вызовы времени. Одни злоумышленники, ощутив падение платежеспособного спроса, поднимают расценки на расшифровку заблокированной информации до 1500 евро (в классификации Dr.Web — Trojan.Encoder.686), другие, поняв, что "пора валить", используют для этого компьютеры жертв (www.anti-malware.ru/news/2015—02-02/15453), третьи ищут места, где еще отсутствуют вирусы и троянцы конкурирующих криминальных группировок.

Естественно, большинство хакеров в поисках хлебных мест еще и еще раз перелопачивают в поисках уязвимостей ОС Windows и приложения, созданные для этой популярной системы. Но есть и первопроходцы Интернета вещей.

В ходе анализа 752 различных устройств, поддерживающих низкоуровневый протокол HART, было обнаружено 29 уязвимостей в компонентах порядка 500 устройств. — www.anti-malware.ru/news/2014—12-02/15107

Вирус можно передать и через электронные сигареты. — www.securitylab.ru/news/462249.php

Были проверены все USB-контроллеры восьми крупнейших мировых производителей: Phison, Alcor, Renesas, ASmedia, Genesys Logic, FTDI, Cypress и Microchip. Хорошая новость в том, что около половины устройств не имеют уязвимостей. Плохая новость: вы не можете сказать, какая конкретно половина. — http://xakep.ru/badusb-v-raznyh-kontrollerah

1800 доменов взломано в результате эксплуатации уязвимости нулевого дня в Adobe Flash Player. — http://blogs.cisco.com/talos/angler-variants

Установив нужное оборудование, можно "видеть" устройства, которые были просто в зоне действия Wi-Fi точки доступа, — даже не подключались к ней. Публичные хотспоты в метро, магазинах и аэропортах — кто контролирует мир? — http://geek-times.ru/post/242979

Кого боятся американские адмиралы? Русских медведей? Исламских террористов?

Начальник отдела морских систем вооружений (NAVSEA) ВМС США вице-адмирал Уильям Хилрайдс заявил, что подлодки типа Virginia уязвимы для кибератак. — http://news.usni.org/2014/10/22/navsea-submarines-control-systems-risk-cyber-attack

"Главная внутренняя угроза, — по словам адмирала, это моряк, который ищет, куда бы подключить свой мобильник и кинуть СМС-ку жене". Ну или незаблокированный USB-порт. — http://breakingdefense.com/2014/10/set-set-cyber-zebra-navy-ship-board-cybersecurity

Но все это пока поиски и концепты. 2014 год ознаменован обнаружением уязвимостей в Linux и появлением значительного — по меркам прошедших лет — количества вредоносных программ для этой ОС, интересом злоумышленников к банкам, системам здравоохранения.

Мир злоумышленников продолжает коммерциализироваться. Началось сращивание киберпреступности и терроризма. Мир стремительно виртуализируется, но его безопасность при этом становится все более хрупкой. Повсеместное понижение уровня понимания "а как это работает" и слепая надежда на новейшие технологии — это страшно. Тем более для людей, которые должны быть уверены в своей безопасности и безопасности тех, за кого они отвечают.

Сколько было надежд на сеть Tor! Но злоумышленники просто регистрировали серверы Tor и инфицировали проходящие файлы, а затем:

Томас Уайт предупредил сообщество о потере контроля над своей серверной инфраструктурой и блокировке учётной записи хостинг-провайдером. Непосредственно перед инцидентом было зафиксировано подключение к серверам неизвестного USB-устройства и открытие корпуса серверов. — http://permalink.gmane.org/gmane.network.tor.user/34619

Кто-то еще полагается на гарантированную защиту данных от любых угроз, если эти данные размещены в облаках?

Прошедший год был отмечен победными атаками шифровальщиков, миллиардными утечками, обнаружением зияющих дыр в ПО — и отказами по их закрытию. Часть пользователей впечатлилась. Но ведь есть еще места, где люди буквально просят прислать им немного вирусов!

"Уже неоднократно говорил — живу без антивирусов примерно с 2002 года. Полёт нормальный. Давно пришло время понять, что все эти „антивирусы" — относительно нечестный способ отъёма денег у малограмотного населения. Любой „антивирус" — ухудшение безопасности (если интересно — поясню)".

Это цитата с одного из форумов. Мнение достаточно популярное, поэтому ссылку не указываем.

Но время идет и

"ма-ма! ☹ кто сталкивался с таким шифровальщиком?"

"П…но тысячи файлов в папках. Первая эпидемия у меня за последние лет 8. Я в неадекватном состоянии, это просто ужас..."

Цитата с того же форума. Причем, судя по обсуждениям, выясняется, что даже если защита и была, то она состояла исключительно из антивируса.

Напуганные статистикой и движимые государственной необходимостью регуляторы всего мира выпускают приказы и разрабатывают стандарты. Ознакомившись с ними и впечатлившись стоимостью и сложностью выполнения требований, потенциальные жертвы атак выстраивают бумажные стены отчетов о своей готовности к бою с любой нечистью.

Гром гремит, но современный мужик даже не собирается креститься. И, к сожалению, данный прогноз сбудется со стопроцентной вероятностью.

В свое время NASA предложило всем желающим поучаствовать в определении задач для марсохода — и было вынуждено закрыть эту инициативу, поскольку большинство хотело устроить "гонки смерти" — загнать марсоход в дюны и посмотреть, что получится. Дальше — больше. Korea Electric Power Corporation, управляющая 23 ядерными реакторами, рекомендовала местным жителям не приближаться к месторасположениям данных АЭС в ближайшие несколько месяцев в связи со взломом неизвестным хакером информационной сети.

PS. Есть подозрение, что когда на Марс проникнет жизнь, то вирусы и там появятся первыми.

PPS. И по результатам расследования инцидента окажется, что на системе защиты решили сэкономить, посчитав, что уж куда-куда, а на Марс вирус не проникнет — там же работают только профессионалы.