Автор: Юрий Ревич © Новая газета РАССЛЕДОВАНИЯ, МИР 3736 23.06.2008, 14:07 185

Бонд морально устарел

На место супермена в спецслужбы пришел хакер.

Небезызвестный экстрасенс Ури Геллер, говорят, умел усилием мысли стирать информацию с компьютерной дискеты. Для того чтобы такое произошло на практике, хакерам-хулиганам, не обладающим эзотерическими способностями, придется как минимум написать программу-вирус. Но они на то и хулиганы, что действуют обезличенно, наудачу: самые популярные вирусы почти все запускаются и распространяются самими пользователями. То есть они не столько используют технические недостатки компьютерных систем, сколько эксплуатируют доверчивость и слабое понимание происходящего со стороны «прокладки между креслом и клавиатурой».

Современная криптография уже давно предоставляет мощнейшие инструменты защиты информации далеко не только соответствующим государственным службам — сейчас каждый может закрыть свою информацию от посторонних глаз так, что получить к ней доступ не помогут никакие суперкомпьютеры. Казалось бы, что спецслужбы должны опустить руки, но не тут-то было: никто ведь и не взламывает защищенные каналы передачи данных напрямую. Пароли доступа крадут из компьютеров с помощью шпионских программ, добывают внедрением агентов, запугиванием или шантажом инсайдеров, выманивают с помощью фишинга (см. «под текст»). Современные шпионы резко отличаются от джеймсов бондов — думаю, что подавляющее большинство сотрудников, например, американского Агентства национальной безопасности (АНБ), никогда не держало в руках пистолета и понятия не имеет о том, как подсунуть подслушивающее устройство супостату.

Все под колпаком

О том, что в шпионских делах техническая составляющая как минимум резко поменяла свой вектор, говорит выход в мае этого года уникальной книги под названием «Шпионское ремесло: тайная история разведтехнологий ЦРУ от коммунизма до «Аль-Каиды». Один из авторов этого труда, Роберт Уоллес, работал в ЦРУ 32 года, причем последние пять лет (до 2002-го) возглавлял департамент технических служб, и предмет знает далеко не понаслышке. Из «Шпионского ремесла» вы узнаете о существовании многих вещей, которые до сих пор казались лишь выдумками авторов триллеров: оказывается, были и сигареты, стреляющие шариками, и надувные самолеты на случай бегства, и дистанционно управляемые роботы-насекомые. Одним из интереснейших направлений, раскрываемых в книге, стало создание в лабораториях ЦРУ таких вещей, как долговечные литиевые батарейки, цифровые камеры и диктофоны, — оказывается, шпионам они стали доступны на десяток лет раньше, чем об этих новинках узнала широкая публика.

ЦРУ долго противилось изданию, но помог новый глава ведомства генерал Майкл Хейден, который слывет реформатором и прекрасно понимает, что почти все изложенные там секреты давно ушли в прошлое. Шпионское оборудование теперь можно приобрести в любом электронном супермаркете, а технические интересы спецслужб давно переместились в область Интернета, сотовой связи и других электронных коммуникаций. Нынешние секреты — это алгоритмы и программы, а не «жучки» и пуговицы со встроенной фотокамерой.

На хакерской конференции, организованной в мае Международной ассоциацией специалистов по радиоэлектронике и электротехнике IEEE, был опубликован доклад, который приоткрывает возможные механизмы деятельности спецслужб в области тотального шпионажа. В работе ученых из Иллинойского университета было показано, как можно построить процессор с простыми и необнаруживаемыми никакими средствами «доработками», позволяющими «знающему человеку» получить доступ к любому компьютеру, как бы он ни был защищен.

Послав на такой компьютер специально сформированный пакет данных по Сети, злоумышленник тем самым активирует «зашитую» в процессор программу. В результате запускается цепочка сложных процессов, которая в конечном итоге позволяет получить доступ к системе по специальному, никому, кроме злоумышленника, не известному паролю. Мало того, после того как такой пароль создан и активирован, все внесенные изменения уничтожаются, и система возвращается к старому состоянию, так что обнаружить сам

факт того, что использовались какие-то инструменты взлома, становится невозможно. Описанный способ взлома необязательно осуществляется через Сеть: можно, например, использовать флешку или компакт-диск.

Аналогичным образом можно запустить троянскую программу для кражи паролей или такую, которая получает доступ к содержимому компьютерной памяти, и вообще осуществить множество типов шпионских атак. Защититься от такого «черного хода» практически невозможно: как показано в работе, модификация затронет лишь несколько тысяч из десятков миллионов транзисторов процессора, и выявить ни тестами, ни даже прямым изучением кристалла под микроскопом наличие «доработки» нельзя.

Так что все держится лишь на нашем доверии к производителям — как вы считаете, способна ли компания Intel (например), которая в настоящее время выпускает восемь из каждых десяти процессоров для персональных компьютеров, пойти на поводу у спецслужб и согласиться на внедрение подобных штучек? Боюсь, что точный ответ на этот вопрос получат разве что наши потомки века через полтора.

Шпионаж и приватность

В 1998 году в России был выдвинут проект «системы оперативно-розыскных мероприятий» СОРМ-2, дополнения к основному СОРМ, касающиеся «сетей документальной электросвязи», т.е. сотовых и интернет-провайдеров. Несмотря на массовую негативную реакцию со стороны общественности (точнее, той части общественности, которая, как говорится, «в теме», простые граждане, кажется, ничего не заметили), 25 июля 2000 года вышел приказ Мининформсвязи №130, который узаконил СОРМ-2. В сентябре 2000 года Верховный суд РФ рассмотрел на предмет соответствия российскому законодательству этот приказ (иск был подан журналистом из Санкт-Петербурга Павлом Нетупским) и постановил, что, во-первых, спецслужбы должны будут предоставить операторам связи всю информацию о «клиенте», во-вторых, лишний раз напомнил, что нарушить тайну переговоров правоохранительные органы вправе только с санкции суда.

Однако 16 января текущего года был подписан приказ Мининформсвязи №6 «Об утверждении Требований к сетям электросвязи для проведения оперативно-розыскных мероприятий», который освободил органы не только от необходимости предоставлять провайдеру информацию о клиенте, но даже информировать о самом факте «прослушки».

Правда, если вы думаете, что российские спецслужбы оригинальны в этом отношении, то ошибаетесь. Американский CALEA («Закон о содействии правоохранительным органам в области коммуникаций»), принятый еще в 1994 году и позднее значительно расширенный, дает спецслужбам ничуть не меньше полномочий, чем российская СОРМ. CALEA дает возможность продолжать прослушивание разговора с участием нескольких человек, после того как объект наблюдения повесил трубку; собирать данные об участниках разговора, даже если они не являются объектами наблюдения; идентифицировать телефонные номера, набираемые после звонка, а также определять местонахождение хозяина беспроводного телефона. Если учесть, что в ряде стран Европы действуют аналогичные законы (где-то помягче, где-то и пожестче), то следует сделать вывод, что понятия приватности в современном мире больше не существует.

Шпионаж и бизнес

Одна из главных тенденций современного мира — это то, что все большие обороты набирает процесс вовлечения спецслужб в круг бизнес-интересов. Не только тысячи бывших сотрудников спецслужб работают в корпоративной сфере по всему миру, осуществляя таким образом слияние частной и государственной разведок, эти разведки начинают сами активно влиять на экономику. Около 95% информации в области экономики собирается из открытых источников. Но оставшиеся 5% нередко представляют собой ключевые сведения, которые могут менять ситуацию в глобальном масштабе, и вот тут-то спецслужбы оказываются на своем месте. Нет, госслужбы — по крайней мере, в развитых странах — не торгуют информацией и не действуют по заказу компаний, просто они исходят из того факта, что в глобализированном мире «национальные интересы» по большей части синоним интересов экономических.

Видимо, впервые тенденция эта проявилась явно, когда в 1990 г. 200-миллионная телекоммуникационная сделка между Индонезией и японской NEC расстроилась, после того как Агентство национальной безопасности США перехватило переговоры участников. В 1994 г. американцы через нашумевшую систему «Эшелон» (существование которой и по сей день, кстати, отрицается) сорвали переговоры между Бразилией и французской компанией Thomson, в итоге 1,3-миллиардный контракт ушел к американской корпорации Raytheon.

И только недавно стало известно, что еще в 80-е годы Канада путем прослушивания ряда посольств США перехватила 2,5-миллиардный контракт на поставку зерна в КНР.

ЦРУ утверждает, что 70% базовых данных для производства микросхем было собрано японской разведкой, что и стало одной из предпосылок становления Японии как ведущей державы в области микроэлектроники.

Говорят, не отстает и Россия, все больше переориентирующая свою внешнюю разведку на экономику, и странно, если было бы иначе, учитывая тот факт, что само государство в лице представителей властных структур у нас является крупнейшим агентом рынка. По мнению западных специалистов, три основных наших ведомства (СВР, ГРУ и ФСБ) уже создали шпионскую сеть, насчитывающую около 100 тыс сотрудников. Вот только почему-то результаты не столь впечатляющи, как в Японии. Видимо, не в одной только информации дело, правда?

Под текст

Такого явления, как фишинг (от английского «рыбалка»), жителям нашей страны пока еще можно не очень опасаться: сам электронный банкинг в нашей стране не настолько развит, чтобы преступникам имело смысл тут что-то ловить всерьез. А вот в странах с развитой инфраструктурой электронных финансовых коммуникаций в последние годы он стал чем-то вроде стихийного бедствия, настолько серьезного, что Microsoft даже озаботилась включением защиты от этой напасти в Vista. А ведь в фишинге вообще не используется практически никаких технических приемов, кроме того, что сайт реально существующего банка или интернет-магазина подменяется ложным, но очень похожим на настоящий. Как вы понимаете, это не требует особых знаний и умений, а все остальное делают сами пользователи, наивно щелкая по ссылке и вводя свои конфиденциальные данные. И хотя общим местом уже стало то, что никакая реальная финансовая контора не будет рассылать по электронной почте просьбы подтвердить свой пароль или ввести реквизиты банковской карты (а вообще, позвонить в банк и проверить — что, сложно?), сам факт, что эпидемия фишинга только нарастает, говорит о прибыльности этого мероприятия.

Автор: Юрий Ревич © Новая газета РАССЛЕДОВАНИЯ, МИР 3736 23.06.2008, 14:07 185
URL: https://babr24.com/?ADE=46312 Bytes: 10608 / 10580 Версия для печати

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта