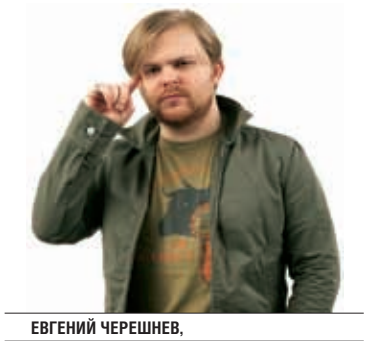


ЕВГЕНИЙ ЧЕРЕШНЕВ,
РЕДАКТОР BUSINESS GUIDE
«ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

УГОВОРЫ НЕ ПОМОГУТ

Наш интерес к информационной безопасности напоминает отношение к ВИЧ: все знают, что он есть, но далеко не всем известны меры предосторожности, кроме использования презерватива. Отсюда и плачевная статистика непобедимости вредоносных кодов.

Между тем истинное положение дел мало кто представляет — массовые атаки ушли в прошлое, а на их место пришли организованные и хорошо финансируемые команды хакеров, чьи подвиги довольно регулярно всплывают в прессе (похищенная недавно база МТС далеко не предел их возможностей). Рядовые пользователи, представители среднего и даже крупного бизнеса порой уверены в том, что причины всех проблем с защитой информации в несовершенстве средств этой самой защиты — криптографического оборудования, межсетевых экранов, антивирусов, операционных систем. Но это не так.

Борьбой с хакерами занимаются лучшие умы планеты — математики, программисты, системные архитекторы, и их усилия, поверьте, отнюдь не тщетны. Сегодня ничто не мешает создать эшелонированную надежную защиту персональных или глубоко конфиденциальных корпоративных данных. Вопрос только в желании, средствах и силе воли.

Но тут мы имеем дело с другой чертой человеческого характера — тягой к самообману. Не секрет, что подавляющее большинство пользователей, установив на компьютер FireWall, моментально чувствуют себя в безопасности, словно бронежилет надели. И, разумеется, сильно удивляются, когда пароль доступа к корпоративной почте оказывается украденным. То же самое касается корпоративного сектора — с поправкой на масштаб защитных периметров. Мы никак не поймем, что безопасность — это не состояние, а процесс. Длительный, сложный, подчас весьма недешевый, но, к сожалению, неизбежный.

Поэтому я не буду говорить о таких тривиальных вещах, как сертификация информационных процессов компании для приведения их в соответствие с международными стандартами безопасности ISO27001. Как показывает практика, обычные уговоры редко приводят к положительному результату. Но если для того, чтобы всерьез задуматься о методах защиты своей информационной собственности, вам требуется пережить взлом бесценной корпоративной базы данных, я вам искренне сочувствую.

КОЛОНКА РЕДАКТОРА

ВИРУСОЛОГИЯ

ЭКСПЕРТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ ЗАЩИТЫ И РАЗРАБОТЧИКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ЕДИНОДУШНО ОТМЕЧАЮТ НЕУТЕШИТЕЛЬНУЮ ТЕНДЕНЦИЮ: ИЗ БАЛОВСТВА И ЛЮБОПЫТСТВА ХАКЕРСТВО ПРЕВРАТИЛОСЬ В ВЕСЬМА ДОХОДНЫЙ БИЗНЕС. 40 МЛН НОМЕРОВ КРЕДИТНЫХ КАРТ, ПОХИЩЕННЫХ В ПОЗАПРОШЛОМ ГОДУ ИЗ ПРОЦЕССИНГОВОГО ЦЕНТРА CARD SOLUTIONS В АТЛАНТЕ (США), СТАЛИ САМОЙ НАГЛОЙ ДЕМОНСТРАЦИЕЙ ВОЗМОЖНОСТЕЙ ХАКЕРОВ, ИСПОЛЬЗУЮЩИХ ПРОРЕХИ В ЗАЩИТЕ КОРПОРАТИВНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ. И ОКОНЧАТЕЛЬНЫМ ПОДТВЕРЖДЕНИЕМ НЕОБХОДИМОСТИ СЕРЬЕЗНОГО, А ГЛАВНОЕ, СИСТЕМНОГО ОТНОШЕНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ЕВГЕНИЙ ЧЕРЕШНЕВ

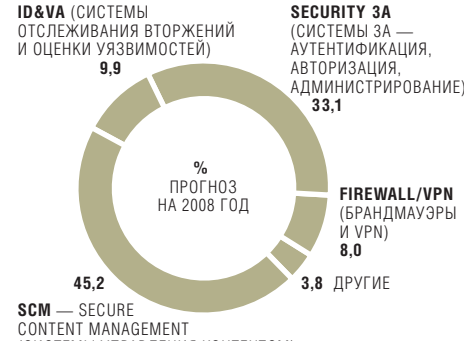
ЗАРАЖЕНИЕ ВЫМЫСЛОМ Экспериментальным путем доказано, что любая система, не защищенная антивирусом и межсетевым экраном (в английском варианте — FireWall), становится инфицированной спустя всего 40 минут после выхода в интернет. Соответственно, уже через несколько дней использования такой компьютер, кишащий сотнями, если не тысячами единиц вредоносного ПО, начинает массово рассылать по всей сети вирусы и спам.

Пользователь же спокойно работает с базами данных, электронной почтой, платными аккаунтами многочисленных сетевых сервисов и не подозревает, что все его пароли уже являются достоянием общественности, а скапливающиеся e-mail с предложениями купить виагру рассылаются с его же компьютера.

А ведь еще несколько лет назад большинство опасных вирусов носило концептуальный характер: программисты-энтузиасты, стремясь прославиться среди себе подобных, пытались максимизировать ущерб, наносимый создаваемыми программами. В результате факт заражения компьютера довольно быстро становился очевидным, и подавляющее большинство пользователей, заметив существенное замедление системы, появление сбоев в работе программ и других подозрительных симптомов, стремилось спешно установить на компьютер антивирус и провести тщательное сканирование.

Сегодня ситуация усложнилась: хакеры и вирус-мейкеры больше не стремятся к публичности, поэтому вредоносные программы зачастую работают по принципу крота — тихо, незаметно, но максимально эффективно.

«Поскольку современные компьютеры стали очень скоростными, пользователь попросту не замечает побочных процессов: рассылка спама, вирусов, украденных паролей и номеров кредитных карт с зараженного компьютера протекает без ущерба для основной деятельности, а следовательно, не побуждает пользователя беспокоиться о собственной безопасности. Этот тренд стал особенно актуальным в последние два года»,— говорит Александр Гостев, ведущий вирусный аналитик «Лаборатории Касперского».



ОБОРОТ МИРОВОГО РЫНКА ПРОГРАММНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИТ-БЕЗОПАСНОСТИ (IT-SECURITY SW)
ПО ДАННЫМ IDC.

Любопытно, что, несмотря крайне высокую активность злоумышленников, о масштабах проблемы осведомлена лишь малая часть пользователей сети — на интернет-форумах, посвященных вопросам компьютерной безопасности, довольно часто можно встретить обвинения разработчиков антивирусного ПО в нагнетании обстановки: мол, компьютер работает без единого сбоя уже пять лет и антивирус мне ни к чему, то есть вирусные эпидемии — вымысел разработчиков, которые борются за расширение рынка.

То есть рост числа зараженных компьютеров связан не только со скептическим отношением пользователей к собственной безопасности, но и с широким распространением пиринговых (P2P) сетей — e-Donkey, KaZaa, Bittorent, а также их аналогов. Работая в этих сетях, пользователи имеют возможность свободного обмена любыми файлами друг с другом. Разумеется, грамотные хакеры практически с момента зарождения P2P-движения стали использовать подобные сети для успешного внедрения троянских вирусов.

Причем, несмотря на то что сегодня многие из P2P-сетей закрыты как противозаконные, на темпах распространения вирусов и спама это не сказалось: охочие до бесплатного ПО пользователи культивируют свободный обмен на сайтах типа www.rapidshare.com и, разумеется, продолжают заражать друг друга и свои корпоративные сети.

AP

ЗАЧЕМ КРАСТЬ КАРТОЧКУ, ЕСЛИ МОЖНО УКРАСТЬ ВСЕ ОСТАЛЬНОЕ

ВИРТУАЛЬНЫЙ МУСОР Многие из нас задаются резонным вопросом: почему нельзя победить тот же спам раз и навсегда? Причин две, и обе они лежат на поверхности.

Во-первых, нельзя уничтожить то, что приносит прибыль, а во-вторых, невозможно сражаться с тварью, которая постоянно регенерирует: вирусы и спам связаны друг с другом, взаимозависимы и, соответственно, нереально живучи. К сожалению, спрос на услуги массовой рассылки существует и он весьма высок.

В феврале 2007 года в Корее арестовали двух спамеров, которые в 2006 году за два месяца разослали в общей сложности 1,6 млрд писем с привлекательными предложениями кредитов под залог недвижимости. Им пришло всего 12 тыс. ответов. Если считать в процентах — невероятно мало, а если в деньгах — довольно прилично: полученную клиентскую базу данных преступники продали заинтересованной компании, оказывающей подобные услуги, за $10–12 тыс. Неплохой доход, не так ли?

Проблема спама сейчас как никогда актуальна. По подсчетам аналитиков «Лаборатории Касперского», порядка 80% всего интернет-трафика нашей страны составляет спам. Огромные вычислительные и сетевые мощности заняты обработкой и передачей огромных куч мусора! В мировом масштабе ущерб в корпоративном и частном секторах исчисляется миллиардами долларов.

Что же касается регенерации, ситуация как нельзя удачно играет на руку злоумышленникам: число пользователей интернета постоянно растет. Только количество Wi-Fi хотспотов в Москве к концу прошлого года перевалило отметку в 1000 единиц, не говоря уже про DSL, EDGE, Ethernet и другие способы подключения к сети. Новые пользователи, как правило, являются дилетантами, поэтому о

СЕГОДНЯ СИТУАЦИЯ УСЛОЖНИЛАСЬ: ХАКЕРЫ И ВИРУС-МЕЙКЕРЫ БОЛЬШЕ НЕ СТРЕМЯТСЯ К ПУБЛИЧНОСТИ, ПОЭТОМУ ВРЕДОНОСНЫЕ ПРОГРАММЫ ЗАЧАСТУЮ РАБОТАЮТ ПО ПРИНЦИПУ КРОТА — ТИХО, НЕЗАМЕТНО, НО МАКСИМАЛЬНО ЭФФЕКТИВНО

РИСУНОК НА ОБЛОЖКЕ: МАРИЯ ЗАЙКИНА