Зомби-генератор в конверте

Спам: минус деньги плюс проблемы

Бурное развитие информационных технологий приводит к все большему смещению бизнес-процессов в виртуальную сферу, а значит, к их ускорению и повышению эффективности работы предприятий. Но не все так радужно. Новая среда рождает не только новые возможности, но и новые проблемы. Одна из них — спам, или, попросту говоря, незапрошенная почта. Если не принять решительных мер по ее отфильтровыванию, «эпистолярная река» может не только вымыть из бюджета фирмы за небольшой срок тысячи долларов, но в отдельных случаях и сделать из IT-структуры организации послушный инструмент чужого бизнеса.

Раз письмо, два письмо...

До сих пор среди руководителей многих организаций бытует мнение, что спам — это не более чем небольшое неудобство — вроде плохой погоды, и к нему должно относиться философски. Но давайте представим, во что обходится это «отделение зерен от плевел» в масштабах организации.

Андрей Никишин, компания «Лаборатория Касперского»

— Люди просто не понимают, что эти 10-15-20 секунд складывается в довольно большое времени, — говорит начальник отдела стратегического развития и аналитических исследований компании «Лаборатория Касперского» Андрей Никишин. — Когда люди отмахиваются от проблемы спама, мне все время вспоминаются слова одного бизнесмена, который сказал: «Когда-то я проводил в самолете около 300 часов в год, а потом узнал про частные самолеты VIP, которые можно заказать в любое время, и лети куда хочешь. Я стал тратить на перелеты втрое меньше времени! И такое впечатление, что у меня в сутках прибавилось 70 минут». Так и со спамом: вроде бы что они — секунды, минуты... А смотришь — целый день набежал.

Опыт показывает, что средний работник, пользующийся одним и тем же почтовым ящиком в течение двух-трех лет, вынужден уничтожать около сотни спамопосланий ежедневно. Сколько нужно времени, чтобы удалить 100 писем, увидев их среди прочей деловой корреспонденции? Допустим, что этот процесс отнимает у него около 10-ти минут в день. Если посчитать, то получается, что в месяц это составляет уже 200 минут, т.е. около 3,5 часов, а в год «набегает» рабочая неделя. При среднем ежемесячном заработке сотрудника в $400 организация теряет в год $100. Представьте, сколько денег вылетает в трубу, если на предприятии работает около сотни человек!

Теперь самое интересное. Такого расточительства можно избежать, потратив на установку и поддержание в актуальном состоянии фильтра спама меньше $1000 в год. Кроме того, во второй год пользования фильтром эта сумма, за счет гибкой политики поставщиков антиспамового оборудования, может сократиться вдвое. Хотя эти подсчеты приблизительные и приведены из расчета использования самых дешевых решений, применение более дорогих все равно дает многократное снижение утечки средств из корпоративного бюджета.

Генеральный директор компании «Ашманов и Партнеры» Игорь Ашманов

Не только информация

То, что спам снижает доходность бизнеса, безусловно, является чрезвычайно негативным фактором. Но не только этим побочным эффектом опасны нежданные послания. В последнее время интернет-сообщество столкнулось с очень неприятным явлением. Спамеры и хакеры все чаще стали объединяться для достижения взаимовыгодных интересов. Суть содружества заключается в рассылке спамерами вирусов, позволяющих при заражении машины превращать ее в управляемый на расстоянии механизм для рассылки писем.

— Нельзя сказать, что данное событие стало для специалистов неожиданностью, — говорит руководитель отдела технической поддержки компании «Антивирусный центр» Николай Ионов. — Скорее стоит говорить о вынужденном переходе спамеров на качественно иной уровень работы вследствие совершенствования технологий борьбы с незапрошенной корреспонденцией.

История рассылки спама прошла несколько стадий. Вначале рассылки производились с личных почтовых серверов. Десять лет назад они воспринимались адресатами спокойно — обратные адреса были реальными, и ни о какой наглости и навязчивости речи не шло. Спамеры начали становиться спамерами в «классическом» понимании этого слова с конца 1990-х годов. Стремясь повысить эффективность рассылок, они принялись разыскивать почтовые серверы, не защищенные от возможности несанкционированной рассылки, т.е. серверы, которые позволяли всем желающим бесконтрольно посылать с них почту. Мерой противодействия этому изобретению стали так называемые «черные списки» серверов, которые поддерживались разного рода общественными организациями либо коммерческими фирмами. Можно было получить конкретный список этих серверов и заблокировать корреспонденцию с адресов, поддерживаемых ими.

Упомянутый выше качественный скачок произошел в 2003 году, когда лавинообразно сформировались сети зомби-компьютеров, принадлежащих подчас ничего не подозревающим пользователям, и применение технологии «черных списков» стало невозможным.

— С конца 2004 года любое профессиональное спамерское программное обеспечение включает специальные модули, позволяющие осуществлять рассылки через зараженные («затрояненные») пользовательские машины, т.е. оно изначально рассчитано на взаимодействие с троянской компонентой различных вирусов, — констатирует генеральный директор компании «Ашманов и Партнеры» Игорь Ашманов.

— Для того чтобы превратить компьютер пользователя в «затрояненную» зомби-машину, ее нужно заразить вирусом, — разъясняет Николай Ионов методику «порабощения» компьютера. — Вирус пишется для конкретной цели. В самом простом варианте он организует на компьютере либо почтовый сервер, либо прокси-сервер, который позволяет удаленно использовать эту машину для рассылок. Точно так же, как клиенты платят спамерам за рекламу, вирусописатель может заплатить спамерам за распространение вирусов по всем адресам их базы. Для чего это нужно? «Чистым» вирусописателям, работающим «за интерес», дается намного более широкое поле для распространения своих творений, потому что рассылка по нескольким миллионам адресов — это все-таки лучше, чем неконтролируемая рассылка, которую делает сам вирус. Другим вирусописателям, склонным обращать свое знание в деньги, это приносит немалую прибыль. Ведь любая машина, на которой «поднят» такой незаконный прокси-сервер, зараженный вирусом, имеет свою цену.

Покупают у вирусописателей возможность использования зомби-машин те же спамеры, либо они попросту вступают с создателями вредоносных программ в бартерные отношения. В среднем только одна рассылка по миллиону адресов обходится клиенту спамера ориентировочно в $100, но, как правило, заказы делаются гораздо более объемные. Если заказываются специфические спам-рассылки, например политические или рассылка того же самого вируса, цена услуги подскакивает до $3 тыс. и выше. Да и стоимость самой зомби-сети не маленькая. Думаем, приведенные доводы и факты говорят сами за себя. Если вы не хотите, чтобы компьютеры вашей фирмы стали инструментом чужого незаконного бизнеса, со спамом надо бороться.

Александр Гудко

(продолжение в следующем номере)