

ИДЕНТИФИКАЦИЯ СПАМА

ЕСЛИ В 2001 ГОДУ ТОЛЬКО ОКОЛО 5% ЭЛЕКТРОННЫХ ПИСЕМ НОСИЛО РЕКЛАМНЫЙ ХАРАКТЕР, ТО В 2007-М ИХ КОЛИЧЕСТВО ДОСТИГЛО 95%. РОССИЯ ПО ИТОГАМ ПРОШЛОГО ГОДА ЗАНЯЛА ВТОРОЕ МЕСТО В МИРЕ ПОСЛЕ США ПО ОБЪЕМАМ СПАМА В ЭЛЕКТРОННОЙ ПОЧТОВОЙ РАССЫЛКЕ. В КАЧЕСТВЕ РАДИКАЛЬНОГО МЕТОДА ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОЙ РАССЫЛКИ РЕКЛАМЫ ПРЕДЛАГАЕТСЯ ВВЕДЕНИЕ ОБЯЗАТЕЛЬНОЙ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ. ОДНАКО У СПЕЦИАЛИСТОВ НЕТ УВЕРЕННОСТИ В ТОМ, ЧТО ЭТИ МЕРЫ СДЕЛАЮТ БОРЬБУ СО СПАМЕРАМИ ЭФФЕКТИВНОЙ.

АЛЕКСАНДР БАУЛИН

НЕСАНКЦИОНИРОВАННОЕ ВТОРЖЕНИЕ

26 января 2007 года в России вступил в силу закон «О персональных данных», регламентирующий порядок электронной рассылки рекламы. Согласно закону, «обработка персональных данных в целях продвижения товаров, работ, услуг на рынке» допускается только с предварительного согласия получателя. Однако со времени его принятия, несмотря на то что прошло уже больше года, объем спама только увеличивается. По данным «Лаборатории Касперского», доля спама в почтовом трафике в России по итогам 2007 года составила в среднем 79,2%, а это второй показатель после США, где законы против спамеров не менее жесткие. Причиной столь высокой доли США в «мусорных» рассылках эксперты называют неспособность пользователей защитить свои компьютеры от проникновения извне.

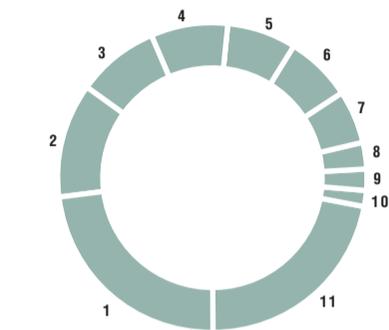
Спам — несанкционированная рассылка рекламных писем — проблема, знакомая каждому интернет-пользователю. 57% американских интернет-пользователей, принявших участие в опросе, проводимом компанией Barracuda Networks (ведущим поставщиком устройств сетевой безопасности для комплексной защиты сети), назвали его самым раздражающим видом рекламы. Для сравнения: назойливость рекламы, рассылаемой обычной почтой, и телефонного маркетинга отметили 31% и 12% респондентов соответственно.

Прямой эффект от рассылки спама — перегруженные серверы и каналы передачи данных и, как следствие, материальные потери. В отчете исследовательской компании Radicati Group отмечается, что в 2007 году только в странах Евросоюза ущерб от нежелательной почты составил \$51 млрд. Российские же компании, по оценке экспертов, потеряли на спаме около \$500 млн.

ПОЧТОВЫЕ ЧЕРВИ По данным «Лаборатории Касперского», в 2007 году число вредоносных программ типа «черви» возросло на 98%. Самого распространенного вида — почтовых червей — стало больше на 36,35%.

Директор по технологиям компании Symantec Оливер Фридрихс назвал развитие червей типа Storm.Worm самой большой угрозой для безопасности систем в 2008 году. Внедряясь в компьютер, они открывают хакеру доступ к личным данным пользователя и рассылают свои копии по другим ПК. Затем сеть из таких компьютеров может быть использована для рассылки спама или организации атак типа DDoS (Distributed Denial of Service). Еще четыре года назад DDoS-атаки совершались хакерами и мелкими вымогателями — теперь же они стали хорошим бизнесом: стоимость проведения подобной атаки сопоставима со стоимостью организации спам-рассылки. В 2007 году они стали особенно популярны среди киберпреступников. В 2008 году, по мнению «Лаборатории Касперского», счет программ класса DDoS пойдет на сотни.

Существуют черви, которые шифруют данные — фото или документы. Способом обезопасить свой компьютер от червей может стать программное и аппаратное шифрование



ИСТОЧНИК: «ЛАБОРАТОРИЯ КАСПЕРСКОГО».

- 1 МЕДИКАМЕНТЫ 23,3
- 2 ОБРАЗОВАНИЕ 11,7
- 3 КОМПЬЮТЕРЫ И ИНТЕРНЕТ 8,7
- 4 ОТДЫХ, ПУТЕШЕСТВИЯ 8,1
- 5 УСЛУГИ ПО ЭЛЕКТР. РЕКЛАМЕ 7,2
- 6 КОМПЬЮТЕРНОЕ МОШЕННИЧЕСТВО 6,9
- 7 ЛИЧНЫЕ ФИНАНСЫ 5,6
- 8 НЕДВИЖИМОСТЬ 2,9
- 9 СПАМ «ДЛЯ ВЗРОСЛЫХ» 2,0
- 10 ПОЛИГРАФИЯ 1,7
- 11 ДРУГИЕ ТОВАРЫ И УСЛУГИ 21,9

документов. Тогда, получив закодированный файл с номером кредитной карты или другими важными данными, хакер столкнется с непростой проблемой дешифровки. Несмотря на длинные ключи ЭЦП, хакеры могут получить доступ к паролям на них в случае ошибок реализации шифрования.

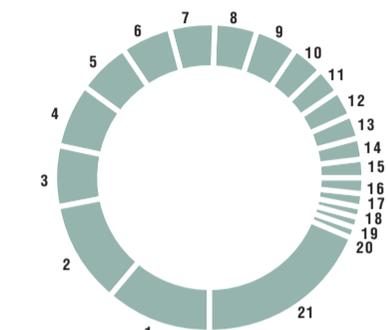
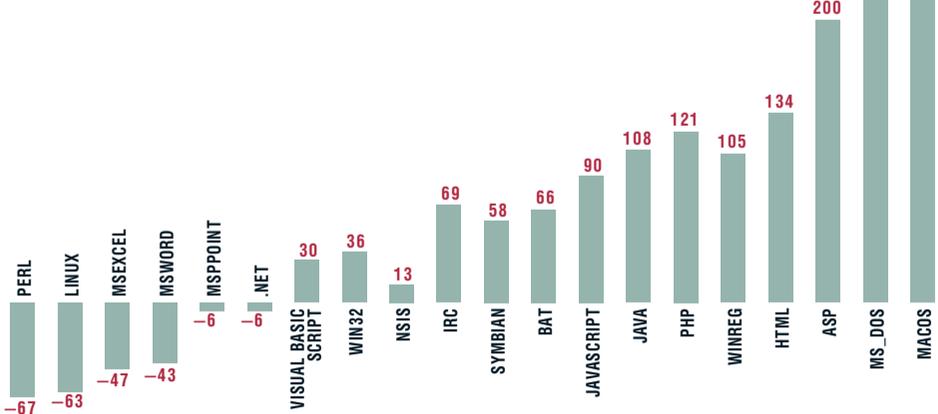
Поэтому для работы в компьютерных системах на государственных предприятиях такие устройства (и соответствующее ПО, если таковое имеется) проходят сертификацию в компетентных органах. Так, реализовано кодирование по ГОСТ 28147-89 электронного идентификатора Rutoken. Производящая его компания «Актив» утверждает, что не только ПО, но и аппаратная часть созданы в России для повышения безопасности систем.

Также популярны программно-аппаратные решения, в которых электронный идентификатор хранит пароли от всех используемых программ, а при изъятии его из ПК доступ к компьютеру блокируется.

Наиболее популярными в России являются устройства eToken компании Aladdin. Включающий радиоиентификационную метку eToken кроме входа в ПК позволяет осуществлять физический доступ в здание. Модели с одноразовым паролем генерируют код, уникальный для каждого промежутка времени — в некотором смысле это аналог смарт-

ТЕМПЫ РОСТА ВО ВТОРОМ ПОЛУГОДИИ 2007 ГОДА ЧИСЛА ВРЕДНОСНЫХ, РЕКЛАМНЫХ И ПОТЕНЦИАЛЬНО ОПАСНЫХ ПРОГРАММ ДЛЯ РАЗЛИЧНЫХ ПЛАТФОРМ (%)

ИСТОЧНИК: «ЛАБОРАТОРИЯ КАСПЕРСКОГО».



ИСТОЧНИК: «ЛАБОРАТОРИЯ КАСПЕРСКОГО».

- 1 США 11,2
- 2 РОССИЯ 10,8
- 3 ПОЛЬША 6,6
- 4 КОРЕЯ 6,4
- 5 ТУРЦИЯ 5,8
- 6 ГЕРМАНИЯ 5,3
- 7 ИНДИЯ 4,7
- 8 ИСПАНИЯ 4,4
- 9 КИТАЙ 4,4
- 10 ВЕЛИКОБРИТАНИЯ 3,3
- 11 БРАЗИЛИЯ 2,9
- 12 ПЕРУ 2,7
- 13 ИТАЛИЯ 2,4
- 14 АРГЕНТИНА 2,4
- 15 ФРАНЦИЯ 1,9
- 16 МАЛАЙЗИЯ 1,6
- 17 КОЛУМБИЯ 1,3
- 18 ЧИЛИ 1,1
- 19 ИЗРАИЛЬ 1,1
- 20 ЕГИПЕТ 1,1
- 21 ОСТАЛЬНЫЕ 18,6

карты с USB-разъемом. В сочетании с правильным ПО такие устройства позволяют пользователю получать защищенный доступ не только к ОС и почте, но и к набору сайтов, все пароли от которых будут зашифрованы в программе с eToken.

Минимальные меры предосторожности от атак спамеров и хакеров — своевременное обновление баз антивируса, установка обновлений операционной системы, а также использование программ типа FireWall. Но даже при полной укомплектованности средствами защиты не стоит открывать подозрительные ссылки, присланные по почте или IM-мессенджерам.

ЭЛЕКТРОННЫЕ МАРКИ Главное, что усложняет борьбу со спамерами, — анонимность пользователей глобальной сети. Что может оперативно предпринять провайдер, выследив злоумышленника? Разве что отключить IP-адрес, с которого производилась рассылка, но ничто не мешает спамеру продолжить ее с другого компьютера и с другого e-mail.

Чтобы не подставлять себя и не светить свой IP, спамеры при помощи вирусов захватывают контроль над компьютерами пользователей, получая не только возможность безнаказанно рассылать рекламу, но и доступ к кон-

фиденциальной информации о частном лице или компании, включая паспортные данные и номера кредитных карт.

Радикальные методы борьбы с нежелательной почтой давно предлагаются ведущими специалистами IT-индустрии. Билл Гейтс, будучи еще главой Microsoft, предложил ввести в оборот электронные марки наподобие почтовых. Добросовестному отправителю каждое письмо обходилось бы в символическую сумму, тогда как злоумышленник, производящий рассылку на сотни тысяч адресов, нес бы серьезные потери. Таким образом, было бы сведено на нет главное преимущество спама — низкая себестоимость. Но под удар попали бы и компании, а также частные лица, по роду деятельности рассылающие большое количество писем.

В России широко обсуждалась идея Евгения Касперского, предложившего разрешить вход в сеть «по документам»: каждому пользователю присваивается уникальный идентификатор, а человека, пойманного на рассылке спама, навсегда «отлучают» от интернета. Для идентификации отправителя можно использовать электронную цифровую подпись (ЭЦП) — фактически очень длинный пароль, подобрать который практически невозможно. Чтобы пользователю не пришлось его запоминать, пароль записывается на USB-брелоке или смарт-карте. Поскольку идентификатор может быть только один, исключается возможность наличия у одного человека нескольких ЭЦП с целью их последующего использования для рекламной рассылки.

Наличие абстрактного идентификатора или электронной подписи позволит отличить нормальное письмо от спама, посланного с поддельного адреса. По замыслу Касперского можно придумать механизм распознавания писем — доверительный центр, где пользователи будут подтверждать, что автор данной ЭЦП не является спамером.

Однако при реализации этой идеи возникнут проблемы как технического, так и этического порядка. Во-первых, велика вероятность того, что со временем появятся инструменты для подделки и кражи уникальных номеров пользователя. Во-вторых, потеря анонимности пугает интернет-сообщество гораздо больше проблем со связью. Евгений Касперский признает, что в текущем виде пользователи ее не примут. Скорее всего, ее реализация возможна только в рамках альтернативной сети, создаваемой, например, для коммерческих компаний, которые ради защиты корпоративных интересов с легкостью пожертвуют анонимностью отправителей. Кроме того, введение этой системы поможет в борьбе с утечкой конфиденциальных данных по инсайдерским каналам: по данным компании InfoWatch, виновниками около 80% утечек являются штатные сотрудники.

Пока личные идентификаторы не внедрены, спамеры озабочены борьбой с провайдерами, безжалостно перекрывающими доступ в сеть компьютерам, с которых производятся массовые рассылки. Более того, провайдер знает физический адрес пользователя с соответствующим IP-адресом, поэтому спамер может оказаться под следствием. Пока чисто теоретически. ■

БОРЬБУ СО СПАМЕРАМИ УСЛОЖНЯЕТ АНОНИМНОСТЬ ПОЛЬЗОВАТЕЛЕЙ ГЛОБАЛЬНОЙ СЕТИ. ВЫСЛЕДИВ ЗЛОУМЫШЛЕННИКА, ПРОВАЙДЕР МОЖЕТ ОТКЛЮЧИТЬ IP-АДРЕС, С КОТОРОГО ПРОИЗВОДИЛАСЬ РАССЫЛКА. НО НИЧТО НЕ ПОМЕШАЕТ ПРОДОЛЖИТЬ ЕЕ С ДРУГОГО КОМПЬЮТЕРА И С ДРУГОГО E-MAIL

