ТЕЛЕКОМ

Опережая хакера

вирусология

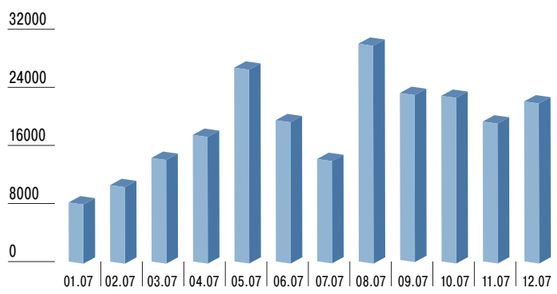
Установленный на компьютере антивирус не делает систему защищенной на 100%. Современные технологии позволяют хакерам легко модифицировать известный вирус до такой степени, что антивирусное ПО перестает его распознавать. Антивирусные компании бьются с этой проблемой, разрабатывая так называемые эмуляторы, которые позволяют определять неизвестные программе вирусы. Какой из представленных на рынке антивирусов лучше справляется с этой задачей, выяснял **Денис Зенкин**.

СЕРГЕЙ МИХЕЕВ

Форматированные жесткие диски, потерянные результаты многих лет работы, украденные пароли к «аське», опустошенный банковский счет… Каких только напастей ни придумают современные вирусописатели, чтобы принять участие в перераспределении материальных благ или просто ради удовлетворения геростратовой мании величия. По данным международного исследовательского центра Computer Economics, в 2006 году ущерб мировой экономики от действий вредоносных программ достиг $13,3 млрд. Действительно, чем больше мы зависим от компьютеров и сетей, тем большее значение приобретает защита от непрошеных гостей из компьютерного андерграунда.

За примером далеко ходить не нужно. Один из самых «выдающихся» вирусов прошедшего года, сетевой червь Storm Worm (также известный как Zhelatin), не раз заставил удивиться даже видавших виды вирусологов. Сотни модификаций этой вредоносной программы демонстрировали редкую изобретательность в выборе поведения, методов самоорганизации, путей распространения и хитростей для обмана пользователей. «Неизвестные авторы реализовали здесь практически все достижения вирусописательской мысли последних лет, многие из которых ранее существовали лишь в концептуальном виде»,— комментирует Александр Гостев, ведущий вирусный аналитик «Лаборатории Касперского». В арсенале этого червя можно встретить смелые идеи по сокрытию присутствия, ухищрения для затруднения обнаружения антивирусами, технологии самоорганизации при помощи создания распределенных сетей зараженных компьютеров и их взаимодействия. Для своего распространения Storm Worm использовал не только традиционные способы, такие как электронная почта и интернет-пейджеры, но и набирающие популярность сервисы эпохи Web 2.0. Копии червя, замаскированные в том числе и под видеофайлы, можно было встретить в блогах, форумах, новостных лентах и социальных сетях.

ДИНАМИКА ПОЯВЛЕНИЯ НОВЫХ ВИРУСОВ В 2007 ГОДУ (КОЛ-ВО ВИРУСОВ)
ИСТОЧНИК: «ЛАБОРАТОРИЯ КАСПЕРСКОГО».



Главная проблема заключалась в том, что практически каждая модификация Storm Worm требовала тщательного анализа и выпуска нового противоядия — обновления антивирусной базы данных. В этой базе хранятся все «отпечатки» известных вредоносных программ. Если в проверяемом файле находится такой «отпечаток», то антивирус сигнализирует о заражении и пытается восстановить данные. Разумеется, анализ и выпуск обновления требовали времени, в течение которого пользователи были беззащитны.

Создается впечатление, что буйству вирусов нет предела — антивирусные компании теряют контроль над ситуацией. В действительности для подобных упаднических настроений нет ни малейшего повода. Несмотря на то что классическое противостояние оружия и брони предполагает временное преимущество первого, современная антивирусная индустрия все чаще опровергает такое представление. Экспертов не первое десятилетие беспокоит вопрос создания проактивной технологии, способной защищать от еще не созданных вирусов. Иными словами, закрывать потенциальную брешь еще до того, как злоумышленники попытаются ее использовать. Однако за это время так и не появилась идея, которая могла хотя бы отдаленно претендовать на звание панацеи. Некоторые технологии оказались достаточно эффективными, но требовали от пользователя недюжинных знаний и потому не получили широкого распространения. Другие помогали только от какого-то определенного типа вредоносных программ. Третьи пали под напором изобретательности вирусописателей, научившихся их обманывать. И все же антивирусы существенно продвинулись: практически все «хулиганские» вирусы сегодня «ловятся» проактивными методами, то есть без выпуска обновлений. Правда, это проблему не решает: за пределами досягаемости остаются самые опасные представители компьютерной «фауны» — вирусы, созданные профессиональными компьютерными преступниками. А именно эти вирусы охотятся за нашими банковскими счетами и секретами.

В сонме перспективных проактивных технологий, способных защитить даже от самых хитрых вирусов, сегодня центральное место занимает антивирусный эмулятор. Хотя этот метод был изобретен еще в 1992 году в России Евгением Касперским, похоже, его время настало только сейчас. Главный недостаток технологии состоит в ее ресурсоемкости: для анализа работы файла в защищенном адресном пространстве компьютера требуется высокая производительность и большой объем памяти. Выполнение этих условий стало возможным только сейчас: современные процессоры достаточно мощны.

Эмулятор представляет собой оптимальный баланс эффективности и дружелюбности. С одной стороны, он способен ловить неизвестные вирусы, «отпечатки» которых отсутствуют в антивирусной базе данных. С другой, он не столь навязчив, как поведенческий блокиратор, не требует сложной настройки и дает минимальный уровень ложных тревог. Это и определяет повышенное внимание к технологии со стороны ведущих разработчиков антивирусов.

По данным компании Perimetrix, почти 100% пользователей используют антивирусные программы. Независимый российский интернет-портал по информационной безопасности Antimalware.ru провел проверку эффективности встроенных эмуляторов. В тестировании участвовали семь популярных в России антивирусных программ: BitDefender Anti-Virus, Dr. Web, ESET Smart Security, Kaspersky Anti-Virus, McAfee VirusScan, Norton AntiVirus, Sophos Anti-Virus. Перед каждой из них была поставлена задача обнаружить 48 тестовых образцов, моделирующих поведение вредоносных программ с помощью эмулятора.

Результаты сравнительного теста антивирусных эмуляторов

Антивирус	Обнаружено тестовых образцов	%
Kaspersky Anti-Virus 7.0	23	48%
BitDefender Anti-Virus 10	20	42%
DrWeb 4.44 beta	12	25%
ESET Smart Security	9	19%
McAfee VirusScan 2007	2	4%
Sophos Anti-Virus 6.0	0	0%
Norton AntiVirus 2007	0	0%

Источник: Antimalware.ru.

Тестирование продемонстрировало преимущество российских технологий. На пьедестал почета попали сразу два отечественных продукта — Kaspersky Anti-Virus и Dr. Web. Первый подтвердил свое реноме изобретателя технологии и доказал, что кому как не «отцу» эмулятора знать, как нужно правильно ловить вирусы. На втором месте неожиданно оказался румынский антивирус BitDefender, который помимо всего прочего отстал от лидера всего на 6%. Недалеко от группы лидеров оказался и популярный в России антивирус американской фирмы ESET. Бета-версия нового продукта компании под названием Smart Security продемонстрировала не самый выдающийся, но тоже неплохой результат. Американские McAfee и Norton в очередной раз доказали, что предпочитают продавать красивую упаковку и бренд, нежели защиту от вирусов. McAfee VirusScan смог поймать лишь 4% образцов, а Norton AntiVirus — и вовсе ни одного. Еще один из участников исследования, английский Sophos Anti-Virus, увы, также обнаружил полное отсутствие способности обнаруживать неизвестные вирусы при помощи антивирусного эмулятора.

Несмотря на торжество российских антивирусных технологий, еще рано говорить, что наконец-то изобретено универсальное лекарство против вредоносных программ. Представленные технологии являются скорее первыми попытками, нежели готовыми к массовому применению идеями. Максимальный результат далек от приемлемого уровня и требует серьезной работы по совершенствованию. Однако уже сейчас можно сказать, что в комбинации технологий защиты от вирусов появился перспективный элемент, способный упреждать появление новых вирусов и быть на шаг впереди компьютерного андерграунда.

СОВРЕМЕННЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ ВИРУСОВ

Сигнатурный метод — реактивная технология распознавания вирусов при помощи их «отпечатков». Каждый штамм анализируется вирусологом, который выделяет его ген, электронный «отпечаток», последовательность байтов и заносит в базу данных. При проверке файла антивирус ищет в нем этот ген и в случае обнаружения сообщает о заражении.
ПРЕИМУЩЕСТВА: возможность «лечения», то есть восстановления зараженного файла.
НЕДОСТАТКИ: требуется время для анализа и создания «отпечатка».

Эвристический анализ — поиск в файлах потенциально опасных команд и их последовательностей.
ПРЕИМУЩЕСТВА: возможность ловить как известные, так и неизвестные вирусы
НЕДОСТАТКИ: недостаточная эффективность, ложные тревоги.

Поведенческий блокиратор — анализ поведения файла в масштабе реального времени. Антивирус следит за операциями каждой программы и сообщает пользователю о подозрительных действиях.
ПРЕИМУЩЕСТВА: 100-процентная защита от всех типов вредоносных программ, в том числе тех, чьи «отпечатки» отсутствуют в антивирусной базе данных.
НЕДОСТАТКИ: требуются глубокие специальные знания, сложная настройка.

Эмулятор — эмуляция работы проверяемого файла в операционной системе. Антивирус создает для каждого файла защищенное пространство, запускает его и следит за его поведением. В случае обнаружения подозрительных действий сообщает о возможном заражении.
ПРЕИМУЩЕСТВА: высокое качество распознавания вирусов, низкий уровень ложных срабатываний.
НЕДОСТАТКИ: ресурсоемкость.

Вирус пошел в нагрузку к жестким дискам

диверсия

Американская компания Seagate в конце прошлого года признала, что часть ее жестких дисков, выпущенных в Китае, была умышленно заражена вирусом. Программа успела поразить всего 300 компьютеров, однако эксперты считают этот акт саботажа показательным. Ущерб от вредоносных программ, расходящихся на физических носителях, в 2006 году в мире составил $1,3 млрд, и потери будут расти по мере распространения ноутбуков и других устройств, использующих портативные накопители информации.

О том, что часть жестких дисков серии Maxtor Basics Personal Storage 3200, выпущенная на заводах китайских подрядчиков компании, заражена вирусом Virus.Win32.AutoRun.ah, заявил в конце прошлого года директор Seagate по корпоративным коммуникациям в регионе EMEA (Европа, Африка, Ближний Восток) Иан О'Лири. Вирус собирал на зараженных компьютерах пароли к играм, в том числе онлайновым, и отправлял их на расположенный в Китае сервер, говорится в заявлении Seagate.

Как отмечают в Seagate, первой факт заражения готовых к использованию съемных жестких дисков (продаются в Евросоюзе по €50–100 штука) выявил летом прошлого года голландский офис «Лаборатории Касперского» (ЛК), в который поступили жалобы от пользователей антивирусного ПО. В результате проведенного расследования выяснилось, что заражена целая партия жестких дисков. Ее размер не смогли назвать ни в российском офисе Seagate, ни в ЛК. Знакомый с ситуацией источник рассказал „Ъ“, что в общей сложности в Голландии было выявлено около 1,5 тыс. зараженных устройств, из которых в продажу поступило около 300. В качестве компенсации Seagate предложила покупателям дисков двухмесячный бесплатный доступ к антивирусному пакету ЛК. Эту информацию подтвердила руководитель пресс-службы ЛК Ольга Кобзарева. «Это наша совместная акция с Seagate,— рассказала она „Ъ“.— Предоставляя антивирусный пакет бесплатно, мы воспринимаем это как промоакцию, направленную на пользователей в Европе».

До последнего времени, как признают эксперты в сфере информационной безопасности, вопрос о заражении ПК через физические носители был неактуален для пользователей и борцов с вирусами. Более 90% вредоносных программ попадало в компьютер через интернет и по электронной почте. Распространение флэш-карт памяти для ноутбуков, фотокамер, сотовых телефонов изменило ситуацию, констатирует глава российского офиса компании Eset Андрей Албитов. По его оценкам, сейчас через устройства памяти проходит менее 10% попадающих в ПК вирусов. Однако перекрыть такой канал заражения сложнее, чем справиться с проникновением вируса через интернет: мешает человеческий фактор. В 2006 году американская компания SNT провела эксперимент: ее служба безопасности разбросала в местах массового скопления своих сотрудников «бесхозные» флэш-накопители с записанной на них программой-шпионом. Почти все они были найдены сотрудниками в день эксперимента и немедленно подключены к компьютерам.

Валерий Кодачигов

Из России со спамом

криминал

Россия впервые заняла второе место в мире в списке стран—распространителей спама, говорится в отчете компании Sophos. Эксперты отмечают, что потери только российских компаний от спама в прошлом году могли достичь $500 млн. При этом бороться с рекламными рассылками в России практически невозможно, поскольку местные интернет-провайдеры не обязаны пресекать эту деятельность.

В отчете Sophos от 11 февраля говорится, что в четвертом квартале 2007 года Россия впервые потеснила Китай, заняв второе место в списке стран—распространителей спама. По данным компании, за отчетный период с территории РФ было разослано 8,3% всей нежелательной почты в интернете. Обгоняют Россию по этому показателю только США — на их долю приходится 21,3%. Третье место, по оценке Sophos, занимает Китай с долей 4,2%. Примечательно, что вклад России в мировую спам-индустрию удвоился по сравнению с третьим кварталом 2007 года — тогда доля страны составляла 4,4%, в то время как с китайских компьютеров поступало 4,9% спама. По данным Sophos, во втором квартале 2007 года Россия занимала восьмое место с долей 3,1%, а годом ранее страны вообще не было в списке стран—распространителей спама. «США и Россия несут ответственность за треть всей нежелательной корреспонденции в интернете. Это не означает, что в этих странах проживает треть всех спамеров мира. Просто в этих странах больше всего так называемых компьютеров-зомби, зараженных специальными вирусами для рассылки спама»,— прокомментировала ведущий консультант по безопасности Sophos Кэрол Терио. По ее словам, эффективная борьба со спамом возможна, если сами пользователи будут следить за безопасностью своих ПК, регулярно обновляя антивирусное ПО.

Несмотря на второе место в мире по числу спам-рассылок, объем рынка спам-рекламы в самой России невелик. По оценкам экспертов, в 2007 году отечественные спамеры получили выручку в размере $13–15 млн. В то же время ущерб от нежелательной почты в разы превышает объем рынка. По оценкам координатора проекта «Антиспам» Евгения Альтовского, российские компании ежегодно теряют на спаме более $30 млн. Гендиректор компании «Ашманов и партнеры» Игорь Ашманов считает, что «эта цифра составляет как минимум $500 млн в год». В Евросоюзе потери от спама в 2007 году составили €51 млрд, говорится в отчете исследовательской компании Radicati Group. «Вероятно, эта цифра несколько завышена, но очевидно, что убытки исчисляются миллиардами долларов. При оценке Radicati Group учитывает стоимость софта для защиты от спама, время, которое сотрудники компаний тратят на удаление нежелательных писем, и другие параметры»,— говорит директор направления аутсорсинга IT-безопасности «Лаборатории Касперского» Андрей Никишин. По его словам, ключевую роль в распространении спама играют не зараженные компьютеры, а хостинг-провайдеры, которых не интересует, чем занимаются их клиенты. «В России один такой хостинг заменяет от 1 тыс. до 10 тыс. зараженных компьютеров»,— поясняет господин Никишин.

Опрошенные „Ъ“ эксперты признают, что в России не работают законодательные механизмы борьбы со спамом. «Есть два закона, направленных в том числе на борьбу со спамом: ФЗ „О рекламе“ и ФЗ „Об информации, информационных технологиях и о защите информации“,— говорит партнер юридической компании „Байтен Буркхардт“ Виктор Наумов.— Но они не работают, поскольку провайдеры не несут никакой ответственности за спам, о чем говорится в постановлении правительства РФ.

Александр Малахов