средствах защиты имеют поверхностное представление — как следствие, имеем весьма высокий риск заражения.

Не стоит забывать и про некоторые аспекты проблемы пиратства. Дело в том, что антивирусные базы компаний «большой российской четверки» — «Лаборатории Касперского», Symantec, McAfee и Trend Micro — обновляются несколько раз в день (в особо критических ситуациях — раз в час). Пользователи, на компьютерах которых работает контрафактное ПО, зачастую лишены самой основы систем защиты — возможности загрузки обновленных антивирусных баз. А поскольку, по данным IDC, на текущий момент уровень пиратского программного обеспечения в общем обороте составляет порядка 80%, рассчитывать на очищение российской части интернета от вирусов и спама пока не приходится.

БАНАЛЬНАЯ БДИТЕЛЬНОСТЬ Да, вирусов не становится меньше. Да, количество спама постоянно растет. Но это не означает, что на рынке нет достойной защиты от этого зла. Напротив, современные отечественные антивирусы от Symantec, «Лаборатории Касперского», Trend Micro, MacAfee — вполне способны обеспечить пользователя достойной защитой. Не стопроцентной, но все-таки довольно высокой.

От пользователя и представителей бизнеса требуется не так много — серьезное и комплексное отношение к проблеме. Отказ от пиратского ПО позволит обновлять антивирусные базы и блок-листы спама по мере их обновления. Разъяснительная работа, проводимая службами IT и информационной безопасности, снизит риск заражения и кражи данных по неосторожности.

И наконец, банальная бдительность, воспетая социалистическим плакатным искусством, отнюдь не является бутафорией. Любопытный факт — для того чтобы смартфон пользователя заразился вирусом Kabir, распространяющимся по BlueTooth, от человека требуется как минимум несколько нажатий «Ok» на предложения соединиться с незнакомым телефоном. Статистика печальна: большая часть граждан, не задумываясь о последствиях, соглашается. То есть, по сути, никто не защитит нас, кроме нас самих.

Разработчики антивирусного ПО стараются сделать процесс общения пользователя и системы защиты максимально простым. В частности, на рынке ощущается довольно явная тенденция перехода от разработки нескольких разносторонних продуктов к одному боксу, сочетающему в себе и антивирус, и сканер, и межсетевой экран (FireWall), и анти-спам. Их задача — обеспечение максимально простой интеграции защитных продуктов в экосистему локальной корпоративной сети и совместимость с другим программным обеспечением.

Поскольку корпоративные клиенты в большинстве своем предпочитают не доверять вопросы безопасности одной компании, что совершенно оправданно, разработчикам приходится довольно усердно работать над программным кодом. Потому что когда хранилище файлов компании защищено антивирусом одного производителя, почтовый сервер — другого, а FireWall, фильтрующий трафик,— третьего, очень важно обеспечить бесконфликтность их работы. Ведь эти программы зачастую борются за одни и те же ресурсы системы, пытаются перетянуть одеяло на себя и иногда считают конкурентное защитное ПО тем самым подозрительным вредоносным кодом. В этом, собственно, и заключается главное отличие пользовательского ПО от корпоративного — в высокой степени корреляции с другими системами для получения максимального эффекта.

AP

40 МЛН НОМЕРОВ КРЕДИТНЫХ КАРТ УКРАЛИ В ПОЗАПРОШЛОМ ГОДУ ИЗ ЭТОГО ПРОЦЕССИНГОВОГО ЦЕНТРА CARD SOLUTIONS В АТЛАНТЕ (США)

МОБИЛЬНАЯ ЧАСТЬ В свое время в печати и электронных СМИ довольно активно обсуждалась проблема грядущего апокалипсиса среди пользователей смартфонов и коммуникаторов. Действительно, не стоит забывать о том, что любой смартфон, по сути, является тем же компьютером — со своей памятью, процессором и даже операционной системой, поэтому в теории ничто не мешает спаму, вирусам, троянам и шпионскому ПО плавно переместиться на мобильные платформы со всеми вытекающими отсюда последствиями. Однако слухи о мобильных эпидемиях довольно сильно преувеличены.

Если бы «умные» телефоны впервые появились в массовой продаже лет десять назад, вероятно, мы бы уже вовсю разбирались с последствиями краж информации и мобильным спамом. Однако последние тенденции в сфере киберпреступлений позволяют говорить о том, что никаких массовых эпидемий не произойдет. Поскольку рынок является самоорганизованным — злоумышленники работают по заказу, четко и узконаправленно, массовые эпидемии им не выгодны в принципе. Их появление повышает шансы обнаружения вирус-мейкеров. Вторая причина — отсутствие достаточного количества самих смартфонов по сравнению с теми же компьютерами — хакерам попросту негде масштабно развернуться. Впрочем, нельзя сказать, что они бездействуют. По данным экспертов «Лаборатории Касперского», сейчас существует порядка 35–40 мобильных вирусов, далеко не все их которых безвредны. Но эта цифра пока не способна состязаться с 200-тысячной вирусной базой для обычных компьютеров.

Однако в недалеком будущем, через три-четыре года, можно ожидать такие же выборочные организованные атаки на конкретные компании и персоналии. Поэтому пользователям мобильных устройств также придется заботиться о своей безопасности.

В ТЕОРИИ Доходы криминального кибербизнеса выходят на уровень, сопоставимый с торговлей наркотиками. И остановить их рост в настоящее время невозможно как минимум по двум причинам. Во-первых, большинство крупных компаний, подвергнувшихся атакам, в целях сохранения собственной репутации зачастую умалчивают о фактах вторжения. Такой подход не может не стимулировать злоумышленников. Вторая проблема фундаментальная: интернет изначально не разрабатывался под столь массовые нужды. Это была сугубо закрытая система, в которой военные и ученые могли свободно обмениваться информацией — никто попросту не предполагал такого массового развития.

В итоге мы получили сотни миллионов, по сути, анонимных пользователей — любой желающий может прийти в питерское интернет-кафе и устроить вирусную эпидемию в Германии. Каждый более или менее подкованный хакер может прикрыться чужим IP-адресом, чтобы взломать банк или базу данных. В сети не предусмотрено никаких процедур персонализации.

В идеале каждый, кто подходит к компьютеру и намеревается выполнить одну из операций в сети, должен представиться — скажем, по рисунку сетчатки глаза или отпечатку пальца. Это нужно для того, чтобы любая операция привязывалась к конкретной персоналии.

В теории эта глобальная и сложная задача вполне реализуема. Но, к сожалению, не на данном этапе развития сети. Однако если противоборство брони и снаряда будет продолжаться теми же темпами, мировое сообщество в течение ближайших пяти лет придет к необходимости весьма существенного пересмотра вопроса присутствия в сети и подхода к информационной безопасности в целом. ■

> НОВАЯ АНТИВИРУСНАЯ КОМПАНИЯ

По оценкам исследовательской компании IDC, рынок антивирусного ПО, чей объем в 2006 году составил около 2,09 млрд. долларов, стабилен и растет не более чем на 10% в год. 80% продаж обеспечивают три крупнейших производителя — Symantec, McAfee и Trend Micro.

Важнейшим событием конца 2006-начала 2007 года для всех производителей антивирусного ПО стал выход новой версии операционной системы от Microsoft - Windows Vista. К моменту начала поставок корпоративных выпусков Windows Vista (30 ноября прошлого года) большинство вендоров не успели обеспечить совместимость своих продуктов с новой ОС. Первой проблемой неожиданно стало наличие в Vista значительно усовершенствованных и переработанных функций безопасности, в частности, технологии защиты ядра операционной системы PatchGuard. Технология PatchGuard, реализованная в 64-битной версии Windows Vista, предназначена для блокирования доступа к ядру операционной системы вредоносных программ. Это вызвало резко негативную реакцию производителей антивирусного ПО, т.к. большинство антивирусов, включая продукты компаний McAfee, Symantec и Лаборатории Касперского, активно используют доступ к ядру для реализации части важных функций. В то же время, в технологии PatchGuard практически сразу после появления предварительных релизов были найдены уязвимости, позволяющие вредному коду отключать или обходить эту функцию. К выпуску окончательной версии корпорация Microsoft устранила обнаруженные «дыры», но вопрос о наличии других потенциального уязвимых мест новой защиты ядра остался открытым. То есть производители антивирусного ПО оказались в проигрыше относительно вирусописателей — вполне возможно, что зловредный код сможет отключать защиту ядра, а борющиеся с ним программы — нет.

Следует отметить, что у некоторых производителей антивирусов, таких как ESET NOD32 и малоизвестный в России Sophos, не возникло проблем с выпуском совместимых с Vista версий, так как в их продуктах не используется прямой доступ к ядру ОС.

Не исключено, что такая политика софтверного гиганта связана с планами отвоевать часть рынка для собственного антивирусного решения, интегрированного с операционной системой — Microsoft OneCare. Антивирус OneCare не встроен в операционную систему, а предлагается по подписке вместе с другими сервисами Windows Live. Выпуск Microsoft собственного антивирусного решения заставил задуматься всех производителей антивирусного ПО — всем памятны примеры постепенного завоевания корпорацией доминирующего положения в различных сегментах рынка даже в тех случаях, когда качество продукта уступало конкурентам. Microsoft воспринимает угрозы безопасности, как главный фактор, заставляющий пользователей задумываться об альтернативных операционных системах, поэтому взять защиту от вредоносного ПО в свои руки выглядит логичным шагом. Пока опасения вендоров оказались преждевременными.

Начало 2007 года ознаменовалось целой серией плохих новостей, связанных с качеством работы нового антивируса. Сначала OneCare провалил два независимых тестирования качества обнаружения вирусов. В тестировании известного специалиста по безопасности Андреаса Клементи, регулярно размещающего результаты тестирования ПО для защиты от вредоносного кода на веб-сайте AV Comparatives, продукт Microsoft оказался худшим из 17- и протестированных. Кроме того, Microsoft OneCare не получил сертификата VB-100, выдаваемого по результатам исследования независимой организацией Virus Bulletin. Затем специалисты сообщили о некорректной работе при сканировании хранилища приложения для работы с электронной почтой самой корпорации Microsoft — обнаружение вируса в письме приводило к удалению или порче всего PST, в котором хранится вся переписка пользователей. Техническая поддержка Microsoft рекомендовала пользователям регулярно создавать резервную копию файла .PST. После такого старта корпорация Microsoft признала, что ее антивирус OneCare требует доработки.

Тем не менее, в будущем, OneCare сможет занять определенную долю рынка. Как и в случае со встроенным в Windows файрволлом, антивирус от Microsoft может оказаться оптимальным выбором для нетребовательных пользователей, не уделяющих безопасности первостепенного внимания. При более основательном подходе к безопасности, например на корпоративном рынке, Microsoft придется конкурировать с традиционными производителями антивирусного ПО на равных.

АНДРЕЙ ВИНОКУРОВ