Автор: Артур Скальский © Lenta.Ru ИНТЕРНЕТ , МИР 3480 22.12.2004, 16:26 267

Состояние дел в современном Интернете можно назвать войной

Несмотря на повальную компьютеризацию последних лет, на свете есть еще немало людей, считающих, что Интернет - это такая программа в компьютере, а вовсе не историческое событие, в корне изменившее структуру мироустройства.

Вместе с тем Интернет - это еще и своеобразное "зеркало общества", только отражает оно не внешний его облик, а внутренний, информационный. Информационное зеркало, как и положено зеркалу, пропорционально отражает все особенности общества, и по мере развития Интернета соотношение "хороших" и "плохих" пользователей оказалось там примерно такое же, как и в мире "реальном".

Что происходит

Люди быстро оценили удобство и оперативность использования Интернета для своих нужд, но оказались плохо восприимчивы к чересчур "техногенной", с их точки зрения, информации о том, что компьютер - это не просто инструмент для эффективной работы, но ещё и "организм", требующий ухода и надзора. С развитием Интернета выяснилось, что этот организм сильно подвержен влиянию извне.

Состояние современного Интернета таково, что компьютер, не защищенный никакими средствами, имеющий в операционной системе "дыру" и выставленный в "открытую Сеть", не простоит и часа, как подхватит какую-нибудь заразу - даже при выключенном браузере и почтовом клиенте, просто через активное интернет-соединение. Виной тому технические просчеты компании Microsoft, создавшей общепринятые сегодня операционные системы. Когда программисты корпорации конструировали эти системы, они решали стоящие перед ними прикладные задачи, не особо заботясь о том, что написанный ими код можно использовать нетрадиционными методами.

Если первые вирусы пытались нанести вред (например, отформатировать жесткий диск), пользуясь штатными методами ОС, то современные вовсю эксплуатируют программные "точки уязвимости". Если раньше основной мотив вирусописателей определялся специалистами по человеческой психике как "самоутверждение", то теперь это главным образом меркантильный преступный интерес, а образ хакера трансформировался из прыщавого подростка, с которым никто не дружит, в квалифицированного "беловоротничкового" бандита, получающего существенные деньги и работающего на крупные криминальные структуры.

Когда в виртуальном пространстве на доминирующий процент "хороших" пользователей оказалось пропорциональное количество "плохих", встал вопрос, который рано или поздно должен был возникнуть: безопасность.

Создать абсолютно защищенную систему или программу очень трудно - если она популярна, найдутся люди, которые будут тщательно проверять её на прочность (заставлять обрабатывать нестандартные запросы, использовать не по назначению различные функции), и, в итоге, во многих случаях находится дыра. Классическая дыра, как правило, позволяет выполнить на компьютере-жертве произвольный исполняемый код - то есть любую операцию. Более сложные системы подвержены риску больше, более простые - меньше. Сложнейшие системы и программы от Microsoft при пристальном изучении оказались просто усеяны дырами, чем злоумышленники и не преминули воспользоваться. Когда стал виден достаточно брутальный характер глобальной вирусной угрозы, в Microsoft не на шутку озаботились и стали придумывать, как дать адекватный ответ хакерам.

Образно говоря, началась война между Добром и Злом. Та же самая, что идёт в так называемом "реальном мире", в который теперь превратился мир, ранее бывший для нас единственным.

Идеологические просчеты

К настоящему времени понятие "программный продукт" из статического превратилось в динамическое - почти каждую программу теперь надо постоянно "обновлять", загружая и устанавливая все новые версии. По мере своего развития программа расширяет функциональность, может переходить из бесплатного состояния в платное и, конечно, закрывать обнаруженные дыры, которые, впрочем, нередко регулярно появляются вновь по мере выхода новых модификаций.

Наиболее критичными являются вопросы защиты того, что соприкасается непосредственно с глобальной цифровой средой - Интернетом, то есть защиты операционной системы и браузера, а также почтового клиента. Раньше наличие у компьютера доступа в Интернет не вызывало никаких подозрений, сейчас, как и в реальной жизни, необходимо "предохраняться" и заботиться о том, чтобы компьютер был огражден от посягательств. А для этого пользователям Windows как минимум нужно иметь последние обновления ОС (в просторечии "заплатки"), классифицированные Microsoft как "важные" или "критические". Они закрывают дыры, которые или уже активно используются распространенными вирусами, или могут быть использованы потенциально. Для установки заплаток надо посещать сайт Windows Update или пользоваться средством ОС, которое само регулярно это делает. Сайт сам определяет, что именно вам обязательно нужно установить, и поддерживает в вашем уме идею о необходимости иметь постоянную связь с корпорацией Microsoft.

Вторая ступень защиты - это так называемый файрвол (англ. firewall - противопожарная перегородка), он же межсетевой экран, он же брандмауэр. В общем случае это особый программный компонент сервера-маршрутизатора или даже специальный компьютер, который устанавливается поперек интернет-канала, чтобы следить за соединениями, которые через него проходят. В зависимости от настроек он может разрешать или не разрешать определенные типы соединений. Как правило, файрволы устанавливают интернет-провайдеры, защищая своих клиентов. Это могут делать и другие коммерческие компании, любые учреждения и вообще любые сети - заодно появляется возможность контролировать трафик и запрещать отдельные сервисы - например, некоторые компании блокируют протокол ICQ, доступ к определённым сайтам (это можно делать по наличию определенных слов в адресе, например, по умолчанию запрещенного почти во всех файрволах слова "sex"). Существуют также "персональные" файрволы, которые можно установить как программу для стандартной ОС. Они часто используются теми, кто экономит трафик, так как позволяют контролировать его и "вырезать" ненужные элементы.

С выходом последнего "кумулятивного" пакета обновлений Service Pack 2 для Windows XP персональный файрвол появился в составе операционной системы. Он - один из модулей "Центра безопасности", который теперь будет являться неотъемлемым компонентом ОС Windows. Корпорация Microsoft строит основы персональной компьютерной защиты на "трех китах" - файрволе, регулярном скачивании заплаток и на обеспечении антивирусной защиты, также постоянно обновляемой. Система теперь умеет думать о том, насколько она безопасна, и бить тревогу, если что-то не так.

Microsoft и появившиеся в больших количествах фирмы, специализирующиеся на интернет-безопасности, изо всех сил стараются донести понимание важности проблемы до широких масс, однако традиционно весьма инертные широкие массы внимать просветителям не торопятся, в результате чего в мире образовалось огромное количество подключенных к Интернету "дырявых" компьютеров, которые легко сдаются рыщущим по сети вирусам и способствуют распространению заразы, что вредит общей стабильности Интернета.

Что они от нас хотят

Что делает современный вирус? Он уже не форматирует жесткий диск. При захвате власти над компьютером он первым делом старается навечно поселиться в системе и почти всегда делает это незаметно для пользователя. Это позволяет ему, запускаясь каждый раз вместе с ОС, постоянно использовать мощности машины и емкость ее интернет-соединения для тех целей, которые определил его автор. Первая цель - это, как правило, размножение. Такие непрерывно лезущие во все щели вирусы получили название "черви". Черви либо рассылают себя по электронной почте, либо непрерывно сканируют Интернет в поисках других дырявых машин. Вторая возможная цель - это ожидание команд из "центра" или выполнение уже заложенных "диверсионных" команд. Задача - превратить пораженный компьютер в "зомби", работающего на вирусописателя.

При достаточно эффективном размножении того или иного вируса он может охватить и превратить в "зомби" значительное количество компьютеров, которые могут составить специальную сеть. Такие сети называются "botnets", и они все чаще применяются в современном мире для совершения киберпреступлений. По команде "из центра" они могут вместе начать выполнение какой-либо единой задачи.

Самыми популярными задачами такого рода сегодня являются рассылка спама, кража интересных хакерам

пользовательских данных, организация "распределенных атак" и распространение других, "расширенных" вредоносных компонентов через сеть Интернет.

Вирус-спамер обычно принимает от "хозяев" базы адресов жертв и "пакеты" предписанного для рассылки спама, содержащего объявления, заказанные клиентами спамерских контор. Как известно, рассылка спама - это сверхприбыльный бизнес, основанный на несанкционированном массовом вторжении в личное информационное пространство отдельных людей. Он широко использует вирусные технологии, ибо на легальных мощностях провайдеров спамерство и хакерство обычно решительно пресекаются. Провайдеры - авангард сил Добра в информационной войне, ибо от качественной работы Интернета зависят их прибыли и правовое благополучие. Тем не менее, всегда существуют плохо защищенные "бесхозные" сети, становящиеся рассадниками заразы, а в некоторых местах мира, где можно легко договориться с местными блюстителями закона (масла в огонь подливает и повальное несовершенство компьютерного законодательства), заразные сети специально строятся и содержатся теневыми структурами.

Вирус-вор ищет на зараженном компьютере информацию, представляющую интерес для злоумышленников. Как правило, это данные о банковских счетах или аккаунтах в платежных системах и коды доступа к ним. В последнее время широкое распространение получил метод "фишинга" (phishing), являющий собой гибрид спамерства и воровства. С помощью спамерских технологий рассылаются письма, притворяющиеся обращениями известных платежных интернет-систем (в том числе систем банков) к своим клиентам. В письме говорится, что банк-де по каким-то причинам нуждается в том, чтобы вы пришли к нему на сайт и ввели логин и пароль. Далее дается ссылка, которая пытается быть похожей на ссылку на банковский сайт, а на самом деле ведет на сайт хакерский. При нажатии на нее пользователь видит перед собой копию реального банковского сайта с формами для ввода логина (номера карты) и пароля (ПИНа). Если он введет их, с ним вежливо попрощаются, а он может попрощаться со своими деньгами. На эту удочку попадается весьма внушительное количество людей, и фишинг распространяется всё более, хотя банки и платежные системы неустанно твердят, что никогда не шлют писем с подобными просьбами своим клиентам.

Вирус-"диверсант" готовит компьютер-жертву и к участию в "распределенной атаке" (DDoS). Такие атаки предназначаются для вывода из строя какого-либо сайта - по команде или в заранее определенное время. Тысячи входящих в botnet компьютеров одновременно обращаются к сайту-жертве с бессмысленными запросами, в результате чего сайт "ложится" и перестает реагировать на запросы "нормальных" пользователей. Такие атаки могут использоваться, например, для шантажа (этим летом поймали группу хакеров из России, угрожавших "завалить" британские онлайновые казино, если им не заплатят денег) и, конечно же, в политических целях. Так, один из любимых объектов DDoS-хакеров - сайт Whitehouse.gov, интернет-резиденция президента США. Не остается без внимания с их стороны и Microsoft.com.

Вирусы же, умеющие подгружать дополнительные модули, могут учинять и вовсе немыслимые вещи, так что даже представить страшно. Поэтому вопросам компьютерной безопасности необходимо уделять самое пристальное внимание. Но, тем не менее, многим владельцам ПК пока это неведомо, и они продолжают раскладывать пасьянсы и играть в "сапёра" на компьютерах-зомби, которые служат делу Мирового Зла.

Черви и шпионы

Если "сканирующие" черви используют "дыры" в операционных системах, то другая разновидность "червей" - почтовая - использует "дыры" в головах. Почтовые черви появились раньше, чем "сканеры", и используют менее совершенную технологию - они приходят в виде писем с некими вложениями и маскируются под "легитимное" письмо, для чего пытаются в поле "от кого" упомянуть какого-нибудь корреспондента из адресной книги пользователя, а в заголовке и теле письма сообщить что-то интригующее, что потенциально должно заставить пользователя открыть прилагающийся к письму файл. Собственно, этот файл и является вирусом.

Так вот, в деле введения пользователя в заблуждение вирусописатели открыли новые горизонты в области массовой психологии и управления сознанием. Здесь даже можно говорить о том, что проблема компьютерной безопасности трансформируется в плоскость безопасности информационной, а оттуда, в свою очередь, - в проблему безопасности едва ли не душевной. И тут даже усматривают богатую почву для научных работ по психологии и психиатрии, так как влияние "манипуляторских" вирусов на сознание масс неожиданно оказалось очень внушительным. В 2000 году вирус "I Love You" нанес мировой экономике ущерб на многие миллиарды долларов, так как маскировался под любовное письмо. Все норовили его открыть, и стремление это было значительно сильнее плохо развитого у масс инстинкта цифрового самосохранения.

Уже упоминавшийся спам сегодня имеет вид не только дурацких писем с ненормальными коммерческими

предложениями, но и вид так называемого "spyware" - "шпионских программ". Они представляют из себя почти те же вирусы, но главное отличие их в том, что они поселяются на компьютерах якобы легально и формально не совершают никаких деструктивных действий. Пользы, впрочем, тоже не приносят, хотя вовсю об этом твердят (профессия такая). На деле они занимаются насильственным показом рекламы, отслеживанием действий пользователя - например, посещений сайтов для выявления рекламной статистики, которая отправляется, опять же, "в центр". "Шпионы" загружают системные ресурсы, и большое их количество на одной машине может напрочь вывести из строя ее операционную систему. Именно "шпионы" ответственны за лезущую на зараженных машинах из каждого угла порнографию и всякие непонятно откуда взявшиеся баннеры.

Что делать?

Специалисты рекомендуют всем пользователям при хождении по Интернету быть предельно бдительными. Рекомендуется воздерживаться от посещений сомнительных сайтов - Интернет делят на "безопасные" и "опасные" зоны (в настройках Internet Explorer есть их описание). Безопасные зоны - "авторитетные" сайты солидных организаций, опасные - всяческий андеграунд с пиратским софтом и нелегальной музыкой, те же порноресурсы и различные виртуальные площадки для азартных игр. Все как в жизни.

Нужно следить за тем, что делается в браузере, и не пытается ли сайт, на который вы пришли, как-то использовать ваш компьютер в неблаговидных целях. Часто характерным показателем неблаговидных намерений является предложение установить какую-то незнакомую вам программу, достоинства обладания которой расписываются в ярких красках - чтобы получить всё это, нужно лишь дать согласие, то есть нажать кнопку "Да". Если вы согласитесь - то будет вам и старт Windows по полчаса, и выпрыгивающие из ниоткуда рекламные окна, и непонятно откуда взявшийся трафик. Так что устанавливать нужно только программы, о которых вы совершенно точно знаете, что они вам нужны и что они произведены "нормальным" производителем.

Как уже говорилось, обязательно нужно обновлять систему и постараться "спрятаться" за каким-либо файрволом. И, безусловно, следует проводить регулярную проверку компьютера на наличие в нем вирусов с помощью антивирусных средств, которые надо также регулярно обновлять. Признанным мировым авторитетом в области антивирусной защиты является российская компания "Лаборатория Касперского", которая также ведет активную просветительскую деятельность. Например, она поддерживает сайт Viruslist.com. Есть и программы для поиска и удаления "шпионов" - одной из самых популярных является бесплатный SpyBot.

И, разумеется, специалисты убедительно просят не покупать то, что рекламируют спамеры - ведь это и есть основная причина, по которой рассылается спам. К сожалению, несознательные люди часто продолжают откликаться на спамерские объявления, хотя многие из них сами заявляют, что ненавидят спамеров.

Всем миром

Вопросы цифровой безопасности в настоящее время сильно заботят коммерческие и государственные структуры. Одной из главных проблем, препятствующих эффективной борьбе со Злом, всегда было несовершенство законодательных норм, не поспевавших за развитием технологий. Проще говоря, до определенного момента хакеры могли творить любые злодеяния и быть абсолютно безнаказанными, так как не было законов, описывающих их действия. Однако сейчас законодатели многих стран, в том числе российские, разрабатывают или уже разработали законопроекты, призванные установить реальную ответственность за хакерство, распространение спама и "шпионов". В США с начала года действует специальный антиспамерский закон "CAN-SPAM Act", недавно закончены разработки закона против spyware. Законы предусматривают за эти действия крупные денежные штрафы или тюремное заключение. Так, в ноябре один из наиболее активных спамеров мира - некто Джереми Джейнс из США - впервые в истории получил за организацию спамерской сети 9 лет тюрьмы. Также этой осенью начался судебный процесс против крупного спамера и распространителя spyware, известного под именем "Spam King" (настоящее имя - Стэнфорд Уоллес). А в минувшее воскресенье Федеральный суд в США установил рекорд по сумме штрафа за спам, обязав три спамерские конторы выплатить пострадавшему провайдеру из штата Айова миллиард долларов.

Развиваются подразделения "компьютерной полиции" - специальных управлений органов внутренних дел, которые ведут борьбу с хакерами и спамерами. В МВД России довольно давно существует Управление "К" (ранее Управление "Р"), ответственное за выявление преступлений в области высоких технологий. В поле зрения таких структур попадают не только хакеры, взламывающие интернет-сети и компьютеры, но и

вредители других коммуникационных сетей - например, сотовых - ведь под угрозой сейчас находится не только безопасность "простых" ПК, но и безопасность карманных компьютеров и мобильных телефонов - всего, где можно выполнить программный код. Особенно это стало актуально при появлении беспроводных стандартов локальной передачи данных, наподобие Bluetooth.

В войне участвуют и крупные компьютерные компании, которые лоббируют законопроекты и проводят специальные акции против вредителей. Как правило, именно коммерческие фирмы являются истцами в судебных делах против спамеров - только что образованный альянс фирм AOL, Microsoft и Yahoo! подал уже несколько сотен исков против разных "произвольно выбранных" отправителей приходящего к ним спама. Производители "софта" и "железа" намерены всерьез взяться и за "шпионов", которые сильно портят им жизнь - подхватившие заразу пользователи нередко звонят в службы поддержки и обвиняют производителей в медленной работе своего компьютера. На прошлой неделе Microsoft объявила о покупке небольшой нью-йоркской компании Giant, производящей антишпионские решения - предполагается, что ее специалисты создадут средства борьбы со spyware, которые также войдут в Windows.

Все больше звучит голосов в пользу того, чтобы положить конец анонимности и информационному беспределу, поместив Интернет и его население в строгие правовые рамки. В качестве одной из главных мер называется введение "электронных паспортов", которые будут однозначно идентифицировать пользователя, чтобы его можно было найти в случае, если он начнет совершать противоправные действия. Если мер не принять, то разгул криминала и онлайнового терроризма может стать катастрофой глобального масштаба. Вирусные эпидемии (о них в наше время узнают из новостей) уже наносят мировой экономике огромный ущерб, так как вызывают остановку или затруднение работы структур, зависящих от использования компьютеров (в современном мире это большинство организаций любого профиля). В начале декабря бывший глава ЦРУ Джордж Тенет назвал Интернет "ахиллесовой пятой США" и "черным ходом" для террористов и врагов. Неделю спустя CSIA - американская ассоциация компаний, специализирующихся на компьютерной безопасности - опубликовала обращение к государственному руководству США, в котором также призвала администрацию Джорджа Буша в кратчайшие сроки самым серьезным образом заняться вопросами национальной безопасности в Интернете. Иначе, по мнению специалистов, враги Америки могут однажды устроить ей "цифровой Перл-Харбор", организовав мощную и неожиданную кибератаку на сети государственного значения.

На фоне этой грозной перспективы не стоит забывать о том, что никто еще пока не отменял применение нечистоплотных кибернетических технологий против отдельных пользователей - существует класс так называемых "троянских" программ, названных по аналогии с одноименным конем. Такие программы, по сути, являются предшественниками spyware, только работают они не на удаленных "рекламщиков", а на кого-то, кто хочет украсть информацию именно у определенного пользователя - например, те же банковские реквизиты, пароли (популярны программы, сканирующие нажатия клавиатуры), а в последнее время нередки случаи, когда мужья с помощью троянов следят за перепиской жен, и так далее.

Информационная война идет, и к ней надо относиться серьезно. Вместе с благами, которые принесли нам новые технологии, пришли и проблемы, и их необходимо в достаточной мере осознавать. Это цена за удобство и эффективность новых методов.

Сергей Рублёв

---

10 самых распространенных вирусов (по состоянию на ноябрь 2004 г.):

I-Worm.Bagle.at 21.39%

I-Worm.Mydoom.ab 11.52%

I-Worm.NetSky.q 8.70%

I-Worm.Zafi.b 7.83%

I-Worm.Netsky.aa 7.33%

I-Worm.LovGate.w 5.69%

I-Worm.Netsky.b 5.39%

I-Worm.Bagle.au 4.89%

I-Worm.Bagle.z 2.90%

I-Worm.Mydoom.m 2.60%

(по данным сайта Viruslist.com)

Автор: Артур Скальский © Lenta.Ru ИНТЕРНЕТ , МИР 3480 22.12.2004, 16:26 267
URL: https://babr24.com/?ADE=18509 Bytes: 22011 / 21943 Версия для печати

эл.почта: babrmarket@gmail.com