Руслан Богатырев

Совершенно секретно, или Всемирная электронная нервная система

Источник: Мир ПК, #04/1998

В прошлый раз наш обзор был посвящен технологии Java; ныне разговор пойдет о неизбежных последствиях информационной революции — об использовании Internet в качестве арены информационной войны с активным применением средств промышленного шпионажа, кибертеррора, "электронного биологического оружия".

Как-то быстро и незаметно пролетела зима, и вот уже за окном все настойчивее стучит апрельская капель. Наше колесо обозрения пустует несмотря на все старания служащих, которые с утра до вечера пытаются вдохнуть жизнь в еще не проснувшийся парк аттракционов. Оно и понятно: кому сейчас захочется испытать на прочность свое здоровье и подхватить какую-нибудь пришлую хворь? Давайте не будем рисковать и продолжим беседу в том уютном ресторанчике, куда мы ненароком забрели зимой.

На этот раз не будем ограничиваться чашечкой экзотического кофе, вызывая недовольство симпатичных официанток. Закажем что-нибудь из того, что есть в меню, но не слишком выделяясь. Скоро к нам подойдет связной из Центра...

Впрочем, мы, кажется, ошиблись лет на пятьдесят. Методы связи, применявшиеся во времена Макса фон Штирлица, все более отходят в прошлое, а шпионы стремительно осваивают новые каналы.

Американцы бьют тревогу

В начале 1998 г. представители ФБР выступили с довольно неожиданным заявлением. По их утверждению, правительства по крайней мере 23 стран наращивают усилия в сфере промышленного шпионажа, направленные против американских компаний. Общие потери США в 1997 г. в области интеллектуальной собственности оцениваются в 300 млрд. долл. Как следует из обзора, подготовленного Американским обществом промышленной безопасности, в 1997 г. было отмечено более 1100 случаев экономического шпионажа. Причем, по словам директора ФБР Луи Фриха, особое внимание привлекали высокотехнологичные фирмы, такие как Boeing, IBM, Texas Instruments, Corning Glass. Наибольший интерес для разведки представляли стратегии в области научных исследований и конструкторских разработок, планы производства и маркетинга, а также списки клиентов различных компаний. Атаки на компьютерные узлы осуществлялись преимущественно через Internet.

Словно подтверждая слова Фриха, один из сотрудников ФБР, Эдвин Фрауманн, опубликовал недавно в журнале Public Administration Review статью, где утверждал, что Германия, Франция, Россия, Израиль, Япония, Южная Корея и особенно Китай активно занимаются промышленным шпионажем против США. При этом среди методов шпионажа все большую роль играют компьютерные. Так, Федеральная разведслужба Германии успешно провела операцию под кодовым названием RAHAB, в ходе которой осуществлялось программное вторжение в различные базы данных и компьютерные системы в США, содержащие информацию по электронике, авиации, химии, оптике, компьютерам и средствам телекоммуникаций. Фрауманн подчеркивает, что разведка и контрразведка Китая, России, Южной Кореи, Японии и других стран активизировали электронный мониторинг не только американских, но и собственных информационных ресурсов, через которые происходит утечка государственных и промышленных секретов.

Озабоченность американцев можно понять: согласно данным Агентства национальной безопасности, США сильнее других стран зависят от сетевой инфраструктуры: здесь сосредоточено более 40% вычислительных ресурсов мира (для сравнения: в России — менее 1%) и около 60% информационных ресурсов Internet. В США сейчас насчитывается более 1,3 млн. взаимосвязанных локальных сетей, а к 2000 г. их количество должно превысить 2 млн.

Ежегодные потери от промышленного шпионажа, в соответствии с отчетами ФБР, составляют от 24 до 100 млрд. долл. По оценкам Отдела науки и техники при президенте США, ежегодный урон, наносимый американскому бизнесу иностранными компьютерными хакерами, достигает

100 млрд. долл. Потери от несанкционированного доступа к информации, связанной с деятельностью финансовых структур США, составляют не менее 1 млрд. долл. в год. Поэтому для успешного развития в рамках Internet электронной коммерции, для организации надежного информационного обмена между государственными органами и осуществления секретных банковских транзакций нужна экстренная модернизация национальной телекоммуникационной и компьютерной инфраструктуры. Одно лишь Министерство обороны США планирует в течение ближайших пяти лет затратить на это около 3 млрд. долл.

В ноябре 1997 г. президентская комиссия США по защите стратегической инфраструктуры представила Биллу Клинтону доклад, в котором предложены меры по защите восьми важнейших "артерий" страны: телекоммуникационных и информационных каналов, сетей электроснабжения, транспортной сети, нефтяных и газовых комплексов, учреждений финансовой и банковской сферы, систем водоснабжения, служб спасения, правительственных учреждений.

Как говорится в отчете, "ныне достаточно обычного ПК и телефонного подключения к Internet, чтобы нанести непоправимый ущерб". Подчеркивается, что отправка по сети определенных команд на центральный компьютер электростанции может привести к таким же разрушительным последствиям, как ее взрыв.

Одно из важных положений этого отчета — настоятельная рекомендация удвоить государственные ассигнования на исследовательские работы в области компьютерной безопасности, довести их в 1998 г. до 500 млн. долл. и обеспечить рост этой статьи федерального бюджета на 20% в год. Агентство национальной безопасности США и Национальный институт по стандартам и технологиям должны создать основу для обмена соответствующей информацией между правительством и промышленностью. Пристальное внимание уделяется и государственной информационной защите частного сектора экономики.

Особо подчеркивается, что детальная информация о национальной информационной инфраструктуре должна быть засекречена, дабы предотвратить возможные террористические акты. Стратегически важные частные компании (прежде всего поставщики доступа в Internet) должны иметь защищенные правительственными структурами каналы информационного обмена. Рекомендуется принять ряд законодательных актов, обеспечивающих защиту информационной инфраструктуры.

Внешние атаки могут преследовать и более серьезные цели, чем пассивный сбор данных, - такие, как, например, выведение из строя главных компьютерных узлов. По мнению экспертов, чтобы парализовать жизненно важные точки созданной инфраструктуры, достаточно нанести удар всего по нескольким десяткам объектов.

Откуда же исходит основная угроза? Частично ответ на этот вопрос дала прошедшая в середине января 1998 г. в Сан-Франциско крупная международная конференция по информационной безопасности (RSA Data Security Conference). Большой интерес вызвало выступление Дэна Нильсена, официального представителя специального подразделения ФБР под названием Центр компьютерных исследований и оценки угрозы инфраструктуре (CITAC). По словам Нильсена, наибольшие проблемы создает халатность системных администраторов компаний, а также сотрудники, принимаемые на временную работу. Немалую опасность представляют и перевербованные "взломщики" и хакеры.

Внешние разведки интересуются, конечно, и военными объектами. По словам официальных представителей американских разведслужб, в 1997 г. был нанесен ущерб более чем 250 компьютерным системам, находящимся в ведении Министерства обороны США. Очевидно, что потери несут и другие страны, однако они, в отличие от США, пока не афишируют свои проблемы.

Разведка и контрразведка

Активизация публичной деятельности ФБР, видимо, связана с намерением оказать давление на американское общественное мнение и стимулировать широкое обсуждение вопросов информационной безопасности. Ряд правительственных органов США заинтересован в получении контроля над информационными потоками. Речь идет о технологии регенерации криптографических ключей (key recovery), позволяющей в случае необходимости расшифровать любую информацию даже без предоставления владельцем исходных ключей. Это очень важный момент, и неудивительно, что глава ФБР тратит столько сил на претворение в жизнь подобного

подхода. Побочный эффект "открытой политики" ФБР — выделение дополнительных субсидий на довольно необычную деятельность: разведку в киберпространстве. В этом смысле Internet мало чем отличается от реальной жизни. Методы разведки и формирования агентурной сети лишь дополняются нюансами опосредованного дистанционного воздействия через компьютерные сети.

Построение сообщества Internet сопровождалось (и сопровождается) внешне благородным лозунгом формирования модели грядущей человеческой цивилизации, которая будет основана на свободе личности, на свободе слова, где голос каждого будет услышан и где наконец установится настоящая справедливость, к которой на протяжении всей своей истории стремилось многострадальное человечество. Но в действительности такое справедливое киберобщество не более, чем утопия: ведь какой бы ни была среда общения — реальной или виртуальной — взаимодействуют в ней живые люди со своими интересами, воззрениями и возможностями, и им есть что терять и что приобретать.

Скорее всего, анархический этап развития Internet вскоре завершится. Хотим мы того или нет, но активное вторжение Сети в нашу жизнь, формирование ранее не существовавших в ней потенциальных источников конфликтов и отсутствие действенных регуляторов, способных обеспечить эффективную защиту общественных и личных интересов, неизбежно поднимут вопрос о гласном или негласном государственном контроле в прямой или опосредованной форме. В игру теперь вступают силы совершенно иного масштаба и уровня подготовки. Они стремятся сохранить свою деятельность в тайне. Но, в отличие от кустарей-одиночек, у них совсем другие цели и возможности. Это разведслужбы.

Доктор Пауль Леверкюн в своих воспоминаниях о службе разведки и контрразведки Германии, опубликованных в 1953 г. [1], писал: "Термин "разведывательная служба" следует понимать в самом широком смысле, т. е. не только как добывание сведений о том, что хранится в тайне от других, но и как изучение того, что открыто выставляется, публикуется и пишется противником". Современные разведслужбы тоже интересуются не только засекреченными, но и незасекреченными данными, причем последними часто больше. Поэтому Internet по достижении определенной степени зрелости начинает представлять колоссальный интерес для разведслужб всех стран мира. По мнению Кристофера Клауса, президента компании Internet Security Systems, лавинообразный рост числа информационных атак обусловлен как раз бурным развитием всемирной Сети.

Диверсионно-подрывная работа

Одной из важных составляющих деятельности разведслужб всегда была диверсионно-подрывная работа. В рамках киберпространства, даже с учетом активности "неконтролируемых" лиц и организаций, происходит постепенный отказ от физического террора (уничтожения компьютерных центров) в пользу "террора" информационного (программных диверсий на уровне блокирования работы устройств, создания узлов-фантомов, ложной маршрутизации и т. п.) [2].

Приведу ряд примеров физического кибертеррора. В ноябре 1969 г. пять членов антивоенной группы Beaver 55 атаковали компьютерный центр в Мидленде (шт. Мичиган) и размагнитили более тысячи магнитных лент. Во время войны во Вьетнаме атаке подвергались компьютеры в американских исследовательских лабораториях, занимающихся разработкой новых видов химического оружия. Хорошо известны факты физических атак на компьютерные центры. Вспомним о взрывах "Красными бригадами" десяти компьютерных центров в Италии (с 1976 по 1978 г.). В марте 1984 г. американская группа United Freedom Front подвергла атаке отделение компании IBM в знак протеста против коммерческой деятельности IBM в ЮАР. В ноябре 1984 г. был атакован офис компании Motorola в Брюсселе. Вслед за этим гремели взрывы на Мальте, во Франции, Англии, Германии, Бельгии, Аргентине, Сальвадоре.

Что же касается информационного кибертеррора, то помимо легендарного американца Кевина Митника известны и другие деятели на этом поприще, многих из которых обвиняли в связи с иностранными спецслужбами. Можно вспомнить американца Герберта Цинна, похитившего в 1987 г. важные файлы из Bell Laboratories и из Центра управления запуском ракет ВВС США; немца Матиаса Шпеера, атаковавшего в 1989 г. ряд американских военных объектов; и еще одного немца — Маркуса Гесса, который вместе с Дирком Бжезински в том же 1989 г. проник в несколько секретных БД в США и Европе.

Изъятием конфиденциальной информации дело, конечно, не ограничивается — происходит и ее порча. Огромная роль в этой деятельности отводится компьютерным вирусам. Ведь именно они позволяют не только успешно преодолевать внешнюю защиту, но и пускать свои "метастазы" в жизненно важные органы компьютерных систем. Проблемы антивирусной защиты осложняются появлением все новых и новых видов киберинфекции. Так, по оценкам ICSA (International Computer Security Association), каждый месяц появляется не менее 200 новых вирусов.

Иммунная система киберпространства

Компьютерные вирусы известны достаточно давно, однако на первых порах их писали в основном кустари-одиночки, для которых это был особый способ самовыражения (а при случае — способ пошантажировать своих недругов). По мере активного развития Internet поражающие факторы вирусов да и скорость их распространения возросли многократно. Теперь исследованием вирусов занимаются многие организации и компании, а системы информационной безопасности даже на коммерческом уровне строят с интеграцией средств контроля сетевого доступа (межсетевые экраны, брандмауэры), криптографических компонентов и антивирусных блоков. Вспомним перестройку в конце прошлого года известной компании McAfee Associates (антивирусные средства), объединившей под новой крышей — Network Associates — фирмы Pretty Good Privacy (криптография), Network General (сетевой контроль) и Helix (администрирование). А в конце февраля 1998 г. в состав Network Associates вошла и компания Trusted Information Systems (брандмауэры, частные виртуальные сети), являвшаяся одним из инициаторов такой организации, как Key Recovery Alliance.

Проблемы информационной безопасности усугубляются не только развитием Internet, но и неизбежной унификацией стандартов компьютерного взаимодействия, а также попытками ряда фирм построить единую операционную сетевую среду, объединяющую миллионы и миллионы компьютеров. Достаточно упомянуть яркую метафору электронной нервной системы (Digital Nervous System), выдвинутую в мае 1997 г. на встрече руководителей ведущих компьютерных компаний президентом Microsoft Биллом Гейтсом. Ее задача — соединить разрозненные программные и аппаратные компоненты с целью добиться автоматической "адекватной" реакции на изменение "показаний датчиков" единого сетевого киберорганизма. В недалеком будущем электронная нервная система сможет опутать своей паутиной все сферы жизни мирового сообщества.

Ассоциация с нервной системой человека не нова. Здесь обязательно нужно отметить концепцию Alife, а также работы исследовательских центров IBM (откуда, похоже, Билл Гейтс и позаимствовал данную идею, развив ее до глобальных масштабов).

Целью Alife является построение искусственной жизни, во многом опирающейся на известные механизмы жизни реальной [3]. Это своего рода "реальная виртуальность", которая противопоставляется более известной "виртуальной реальности". В последние годы большие успехи уже достигнуты в таких направлениях Alife, как нейронные сети и генетическое программирование.

Но уж коли разговор зашел о разведслужбах, стоит упомянуть так называемую иммунную систему киберпространства (Immune System for Cyberspace, ISC), действующий макет которой был продемонстрирован специалистами IBM в октябре прошлого года на проходившей в Сан-Франциско крупной конференции Virus Bulletin'97.

Антивирусная технология IBM [4] построена на основе модели иммунной системы человека и опирается на четыре важных принципа. Первый — наличие так называемого врожденного иммунитета, способствующего выявлению большого количества ранее неизвестных "микробов" всех видов (поражающие механизмы для файлов, для загрузочных секторов, макровирусы). Второй — формирование адаптивного иммунитета, позволяющего вырабатывать нейтрализующее средство при первом же появлении новой инфекции. Третий — быстрое распространение полученного лекарства на миллионы пораженных болезнью компьютеров. Четвертый — обеспечение высокой эффективности вакцинации и лечения за счет полной автоматизации этого процесса. Система ISC (см. рисунок) предусматривает распределенную работу с использованием центра "лекарственных препаратов". Удаленные программные агенты выявляют факт проникновения инфекции и при невозможности справиться с неизвестным микробом собственными силами сигнализируют об этом в центр. При этом берется проба "микроорганизма" для приготовления вакцины либо лекарства, которые без участия человека внедряются в пораженный компьютерный организм.

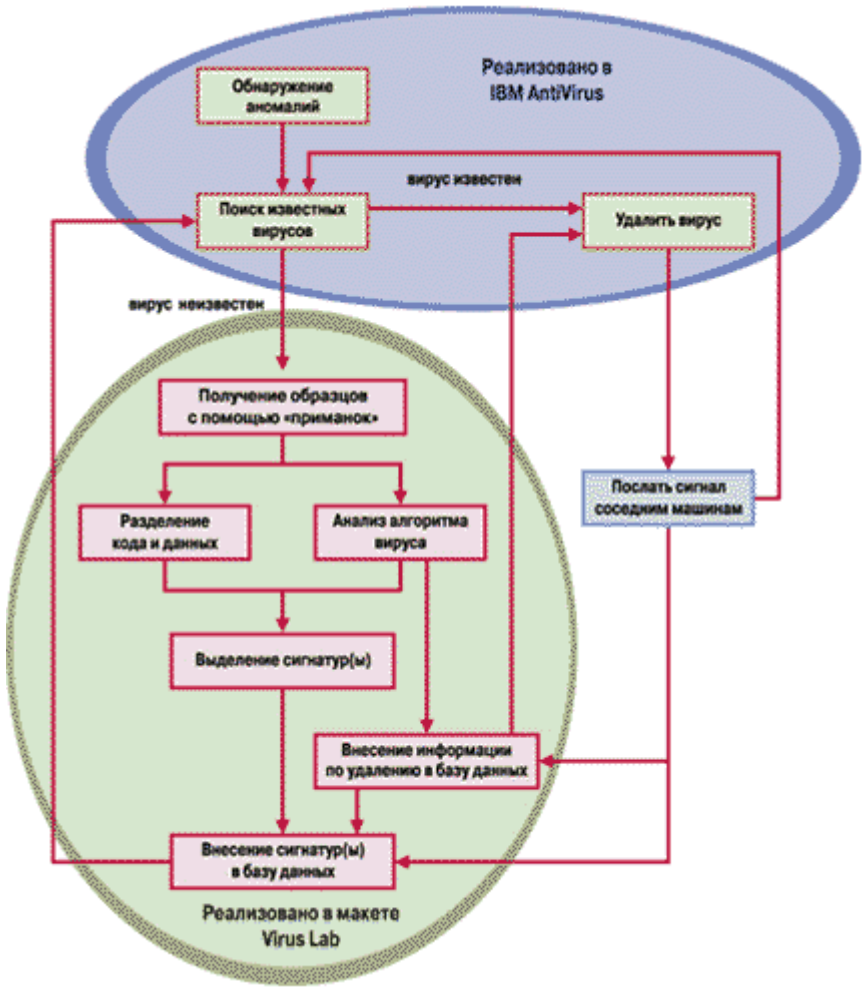

Рис. 1. Структура иммунной системы IBM

Несмотря на наличие нескольких патентов, непосредственно касающихся ISC, работа пока не завершена. Еще требуется "довести до ума" транспортный механизм, обеспечивающий надежный и быстрый обмен информацией между клиентским компьютером и "центральной диспетчерской", а также добиться эффективной вакцинации. Очевидно, что успехи в развитии ISC не ограничатся одним лишь пассивным излечением пораженных участков компьютерного организма, а позволят получить изощренный механизм контроля и воздействия на миллионы компьютеров.

Борьба с киберинфекцией строится по принципам, известным современной медицине: согласно учению И. П. Павлова, реакцией организма на вторжение инфекции управляет центральная нервная система. Неудивительно, что разработки компьютерных ученых столь близки этим открытиям [5]. Авторы новых средств антивирусной безопасности все чаще обращаются к решениям, достаточно хорошо проработанным в таких направлениях медицины, как эпидемиология и иммунология.

Трансформация операционной среды компьютеров в некое подобие живого организма наводит на мысль о создании электронного "биологического оружия" неограниченного радиуса действия. С появлением компьютерной иммунной системы следует ждать возникновения и разрушающего ее компьютерного СПИДа, причем в самых неприятных его вариациях.

Акцентируя внимание на вирусах и иных средствах информационного воздействия, вряд ли стоит чересчур драматизировать ситуацию. В то же время недавние события показывают, что проблемы существуют и игнорировать их уже нельзя. В конце февраля 1998 г. целенаправленной атаке подверглись компьютерные сети Пентагона, причем по всей видимости это был отвлекающий маневр с целью выявления реакции на подобные вторжения (официальные лица списали все на обычное хулиганство двух 15-летних подростков, уже задержанных сотрудниками ФБР).

В начале марта Космический центр им. Кеннеди, региональные отделения NASA, подразделения ВМФ США, несколько крупнейших американских университетов (MIT, Калифорнийский университет в Беркли), а также ряд государственных учреждений США подверглись атаке хакеров. Результатом вторжения явилась принудительная перезагрузка компьютеров. Были использованы изъяны в ОС Windows 95 и Windows NT, известные под названиями New Tear, Tear Drop II и Boink. Предполагается, что данная атака была приурочена к выступлению Билла Гейтса на мартовских слушаниях в Сенате США по вопросу о монополизации Internet. Инициаторы атаки явно преследовали цель дискредитировать Microsoft и показать уязвимость повсеместного распространения единой операционной среды.

Стратегия и тактика информационной войны

Мы подошли к вопросу о принципах ведения информационной войны в современных условиях. Как известно, одна из важнейших задач любого государства — борьба за контроль над информацией. Мы не будем касаться психотронного оружия, психотропного оружия, генераторов пси-полей, оружия на основе электромагнитных импульсов, инфразвука и радиоволн — сосредоточимся лишь на информационной войне.

Информационная война — это не то же самое, что война электронная. В ее основе лежат главным образом психологические и мировоззренческие факторы, а также, естественно, компьютерные технологии. Однако было бы неверно сводить информационную войну к идеологии и пропаганде: это понятие куда более широкое. Ныне аббревиатура IW (Information Warfare) становится все более и более распространенной. В конце 1996 г. Роберт Банкер на одном из открытых симпозиумов представил доклад, посвященный новой военной доктрине вооруженных сил США XXI столетия (концепции Force XXI). В ее основе лежит разделение всего театра военных действий на две составляющих — традиционное пространство, населенное людьми, и киберпространство, причем последнее имеет более важное значение. Банкер предложил доктрину киберманевра, которая должна явиться естественным дополнением традиционных военных концепций, преследующих цель нейтрализации или подавления вооруженных сил противника.

Таким образом, в число сфер ведения военных действий, помимо земли, моря, воздуха и космоса теперь включается и инфосфера. Как подчеркивают военные эксперты, основными объектами поражения в новых войнах будут инфраструктура и психология противника. Физическая оккупация территории не понадобится. Размывается и само понятие победы: таковой считается подавляющее превосходство в информационном контроле.

Информационная война может перерастать в непрерывную борьбу, способную в скрытой форме продолжаться многие годы. При ее подготовке удастся в скором времени выйти на такой уровень, когда новые информационные технологии (и не только в области криптографии) будут приравниваться к сведениям государственной важности.

В известном меморандуме Клинтона и Гора, выпущенном в 1993 г., с которого, собственно, и начала свою жизнь Национальная информационная инфраструктура (NII), говорится о том, что стратегической целью США является "достижение мирового лидерства в фундаментальной науке, математике и технике" [6]. Последовательно претворяя в жизнь идеи NII, в конце февраля 1998 г. генеральный прокурор США Джанет Рено объявила о создании Центра по защите национальной инфраструктуры (National Infrastructure Protection Center). Наращивая отрыв в технологическом превосходстве и создавая компьютерный щит, Америка неуклонно идет к поставленной цели.

Литература

1. Итоги второй мировой войны. М.: Иностранная литература, 1957
2. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. НПО "Мир и семья - 95", 1997
3. Богатырев Р. Этот странный придуманный мир // Компьютерра. 1997. # 30, 32, 33.
4. Kephart J. A Biologically Inspired Immune System for Computers. IBM Thomas J. Watson Research Center, High Integrity Computing Laboratory, 1994.
5. Kephart J., Sorkin G., Chess D., White S. Fighting Computer Viruses // Scientific American, November 1997.
6. Богатырев Р. Дорога в будущее, или Планета Internet в созвездии Белоголового Орла // Планета Internet. 1996. # 2.