Ботнет — зомби у Вас на столе

Ботнеты, или сети зараженных компьютеров, обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, взлома паролей на удаленных системах, DDoS-атак.

Дмитрий ЛАНДЭ

В начале эры персональных компьютеров появились и первые компьютерные вирусы. Механизм их работы и распространения был прост: при попадании в память компьютера они решали две основные задачи — размножения и выполнения действия, заложенного их создателями (иногда этим действием могла быть невинная шутка, иногда — умышленное зло).

Безусловно, существовали и другие вредоносные программы, например, так называемые трояны, которые, попав на компьютер, никак себя не проявляли, а как бы затаившись, ожидали наступления некоторых условий и только тогда выполняли действия, предусмотренные их авторами.

Развитие сетевых технологий, реализация известной идеи, что сеть — это компьютер, породили следующее поколение вредоносных программ — «червей». Точно так же, как вирусы внутри компьютера, черви размножаются в сети, оставляя свои копии в памяти многочисленных компьютеров. «Простые» черви работают по заранее задуманному авторами сценарию, размножаясь, разрушая, атакуя, рассылая угрозы и спам. Черви — это «челенджеры», автопилоты с заданной программой действий, которые успели нанести немало вреда. Однако мир не стоит на месте. Плохим ребятам захотелось управлять червями, заставлять их по команде выполнять те или иные действия на зараженных компьютерах, менять задания и сценарии работы. Оказалось, что не только хакерам нужны атаки на чужие серверы, коды чужих кредитных карточек или рассылка спама. Хакеры стали находить заказчиков (или заказчики — хакеров) и продавать им управление сетевыми червями. За деньги, разумеется.

Итак, мы и подошли к теме статьи — ***ботнетам***, слову, образованному от английских слов «робот» и «сеть». Такое имя получили сети зараженных компьютеров, централизованно управляемых владельцами (или арендаторами).

Ботнеты могут управляться не только централизованно. Наиболее изощренные из них поддерживают связь друг с другом, передают команды от хозяев децентрализованно в соответствии с идеологией пиринговых сетей*). В настоящее время совокупная вычислительная мощь некоторых ботнетов в разы превосходит самые мощные суперкомпьютеры.

> Ботнет — это компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами — автономным программным обеспечением. Чаще всего бот в составе ботнета скрытно устанавливается на компьютере жертвы и позволяет злоумышленнику выполнять некие действия с использованием ресурсов зараженного компьютера и его программным обеспечением. Обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удаленной системе, атак на отказ в обслуживании (DDoS). (Википедия)

По словам вице-президента компании Google Винта Серфа (Vint Cerf), к Интернету подключены более 600 млн. компьютеров, из которых около 150 млн. являются участниками ботнетов

*) Детальнее о пиринговых сетях можно почитать в статье Дмитрия Ландэ «P2P — по секрету всему свету…» («СиБ», 2008, № 2, с. 104–110).

Управление в ботнетах обычно получают в результате установки на зараженных компьютерах необнаруживаемого пользователем программного обеспечения. Это совершают путем:

• заражения компьютера вирусом через уязвимость в программном обеспечении;

• использования невнимательности пользователя (маскировка под «полезное содержимое»);

• перебора вариантов администраторского пароля к сетевым ресурсам — преимущественно в локальных сетях.

Создатель Интернета, изобретатель стека протоколов TCP/IP, а сегодня вице-президент компании Google Винт Серф (Vint Cerf) на Мировом экономическом форуме, прошедшем в 2007 г. в Давосе, представил статистику по распространенности ботнетов. По его словам, тогда к Интернету было подключено более 600 млн. компьютеров, из которых около 150 млн. были вовлечены в ботнеты.

Основными средствами рассылки спама в Интернете, хакерских атак на серверы сегодня являются бот-сети. Естественно, большинство пользователей зараженных машин даже не догадываются о том, что их компьютеры используются для организации распределенных атак, рассылки спама и прочих злонамеренных акций, например, фишинга (размещения сайтов, имитирующих реально существующие ресурсы с целью хищения конфиденциальных данных). И что самое ужасное, в число таких зомби может входить и компьютер, мирно дремлющий на письменном столе у Вас, читатель.

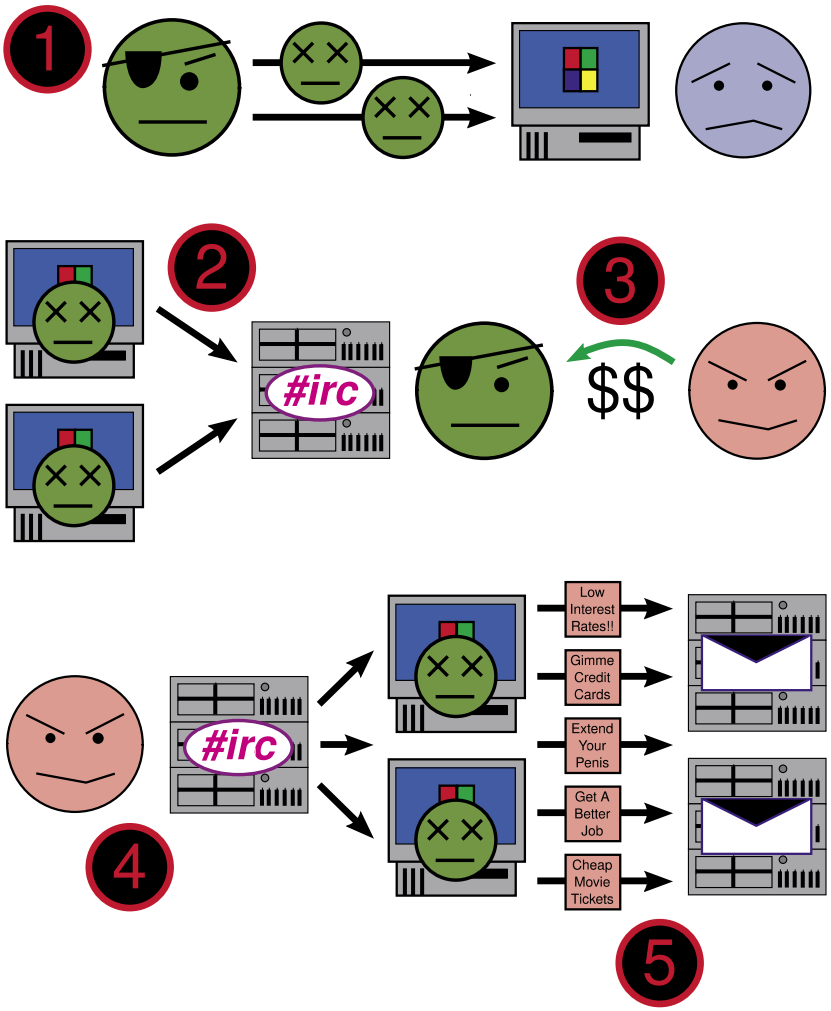

Схема взаимодействия участников ботнет-бизнеса: 1 – хакер заражает компьютеры; 2 – зараженные компьютеры «слушают» команды управления; 3 – хакер получает деньги от заказчика за аренду ботнета; 4 – заказчик управляет ботнетом; 5 – ботнет рассылает спам

По информации Washington Post, в настоящее время изменилась временная динамика активности хакеров, которая раньше приходилась лишь на ночи в выходные. Сегодня хакерские атаки часто проводятся в будни, что свидетельствует о том, что создание и эксплуатация ботнетов превратилась в основное занятие достаточно большого числа людей. Похоже, ботнеты действительно популярны в определенных узких кругах. Время от времени в блогах появляются объявления типа «сдам в аренду ботнет для рассылки спама — 15 тысяч машин на dsl-канале желательно 70% он-лайн 24/7 — за 4000$ в сутки, тестовое использование в течение 4 часов бесплатное». Некоторые менее мощные ботнеты предлагают на других условиях — за час атаки просят $20, а за сутки — в среднем $100.

В Википедии приведена схема взаимодействия участников ботнет-бизнеса (**рис.**).

Представленную схему можно дополнить еще использованием бот-

Минное поле современного Интернета

Алексей Гребенюк, специалист по информационной безопасности

— Современный Интернет напоминает минное поле, где пользователь на каждом шагу сталкивается с риском вирусного заражения своего компьютера или может стать жертвой сетевых мошенников.

Не секрет, что бреши в системе безопасности подчас очень дорого обходятся пользователям. По информации консалтинговой группы Deloitte, 18% финансовых компаний стали жертвами утечки конфиденциальной информации. При этом они признались, что утечка повлекла за собой и материальные потери.

Как показывает практика, «сломать» можно практически любую систему. Сегодня под прицел хакеров попадают серьезные организации. Даже в компьютерной системе Министерства внутренней безопасности США в июне 2007 года были обнаружены вредоносные программы, которые похищали пароли.

На днях мир отметил печальную годовщину — тридцатилетие спама. Пройдя путь от надоедливой рекламы американских консервов Hornel Foods под торговой маркой SPAM, рассылка нежелательных писем превратилась в серьезную общемировую проблему.

Это связано с тем, что для организации массовых рассылок спама все чаще используют вычислительные мощности компьютеров пользователей путем несанкционированной установки прокси-серверов, программ, самостоятельно осуществляющих рассылку спам-корреспонденции, таких, например, как Trojan.Spambot. Постоянная перекомпиляция исходных текстов затрудняет детектирование вредоносных программ данного типа антивирусными средствами.

Для установки на компьютер пользователя программы Trojan.Spambot применяются различные варианты схем с использованием одиночного загрузчика с последующей регистрацией Trojan.Spambot в секции автозагрузки. Возможны варианты использования двухкаскадных загрузчиков, когда один загрузчик скачивает другой, и уже потом устанавливается Trojan.Spambot. Применяются также схемы «дроппер–загрузчик», «загрузчик–дроппер», внедрение в Explorer и другие процессы.

Многие из нас замечают странные утечки трафика, а наши почтовые ящики почти на 90% переполнены совершенно ненужной и раздражающей информацией. Одной из причин такого невиданного уровня спама как раз являлся Win32.Ntldrbot (Rustok.C).

Главным событием мая стало обнаружение специалистами антивирусной лаборатории компании «Доктор Веб» неуловимого Win32.Ntldrbot (aka Rustock.C) — вируса, который смог выстроить из заражаемых им компьютеров огромную бот-сеть. По оценке компании Secure Works, бот-сеть, созданная Rustock, стоит на третьем месте среди крупнейших бот-сетей и способна рассылать ежедневно до 30 миллиардов спам-сообщений.

Главная тенденция в мировой паутине — бизнес, построенный на компьютерной преступности и краже конфиденциальной информации, поскольку ушло в прошлое время вирусописателей-романтиков. Цель этих людей — получение прибыли, и создание бот-сетей — одно из самых перспективных направлений в этом криминальном бизнесе.

Для этого все способы хороши, и пользователю ни в коем случае нельзя забывать про фишинг. Спам становится все более насущной проблемой в основном из-за фишинга. По мнению некоторых специалистов, от 20 до 30% спама в настоящее время является фишингом, в котором у адресатов пытаются «выудить» важные личные или финансовые данные. При этом его доля даже в спаме постоянно растет.

По мнению исследователей CipherTrust, показатель реакции получателей на фишинг-сообщения значительно превышает уровень ответов на «классический» спам. Несмотря на постоянно растущий объем спамерских рассылок, усовершенствуемые антиспамерские фильтры все успешнее отсеивают спам. Однако фишинг-атаки достаточно хорошо замаскированы, всегда социально ориентированы и все возрастающий их процент проходит сквозь барьеры. В связи с этим и ответная реакция находится на гораздо более высоком уровне.

Таким образом, на сегодня мы вынуждены констатировать: не только защита строится на принципе комплексного подхода — его с таким же успехом используют и киберпреступники. Однако не следует забывать, что борьба с новыми угрозами не останавливается, и радует то, что представители компаний из СНГ — в числе технологических лидеров борьбы с фишингом и бот-сетями.

нетов хакерами, неспособными создавать собственные бот-сети, а ворующие их у своих же коллег. Для осуществления подобных махинаций разработаны многочисленные хакерские утилиты.

Учитывая количество зараженных компьютеров, входящих в подобные зомби-сети, можно лишь догадываться, каков денежный оборот в этом бизнесе. По оценке ФБР, экономический ущерб от деятельности операторов ботнетов превысил $20 млн. Другую, на порядки большую цифру привел Гади Эврон, известный израильский специалист по информационной безопасности, оценивший доходность сетей компьютеров-зомби в 2006 году в $2 млрд. Владельцы ботнетов, по его сведениям, в основном зарабатывают на фишинге, рассылая миллионы электронных писем-завлекалок. Трафик от пользователя к «подставному» сайту все чаще проходит через ботнет, что позволяет обойти защиту браузерных антифишинговых систем. Главной целью атак остается финансовый сектор, а самыми популярными логотипами фишеров по-прежнему являются eBay и PayPal.

В течение последних нескольких лет атаки, вызываемые ботнет-червями, становятся уже привычными. Однако не всегда сообщается, что в атаках участвуют ботнет-структуры.

Чаще всего, управление ботнетами производится по IRC-протоколу. Вирус инсталлирует программу-робота, которая через заданные промежутки времени обращается к одному или группе IRC-серверов за командами ботмастера — администратора ботнета. До момента использования вредоносная программа «спит» и ждет команды. Получив команду от хозяина ботнета, зараженный компьютер начинает ее исполнять. В ряде случаев по команде загружается исполняемый код, благодаря чему имеется возможность «обновлять» программу и загружать модули с произвольной функциональностью.

Традиционная схема предусматривает взаимодействие всех ботов с одним центральным звеном, что делает сеть уязвимой, поскольку удаление сервера полностью нейтрализует ботнет. Однако в декабре 2006-го специалисты SecureWorks обнаружили нового «троянца» — SpamThru, который объединяет компьютеры-зомби по принципу децентрализации. В создаваемом таким образом ботнете каждый участник получает информацию о других «сотоварищах», и если управляющий сервер вдруг отключается, достаточно дать одному из ботов координаты нового источника команд, чтобы возобновить работу.

В последнее время стали известны технологии управления ботнетами через ICQ, веб-интерфейс и даже через SMS. Так, например, ботнет MayDay использует стандартный протокол HTTP, который отправляется через прокси-серверы. Этот прием позволяет вредоносной программе обходить системы безопасности, используемые многими крупными компаниями.

Так в апреле 2008 года на конференции RSA представители исследовательской компании Damballa рассказали о новом гигантском ботнете Kraken. Он насчитывает более 400 тысяч зомби-машин, в числе которых оказались компьютеры сетей 50 компаний, входящих в список Fortune 500, причем на 80% машин было установлено антивирусное программное обеспечение. Для приема управляющих команд этим ботнентом используется специальный внутренний протокол, работающий поверх UDP и TCP, причем передаваемые данные подвергаются шифрованию. Кроме того, при утрате работоспособности управляющим узлом зомби-хост автоматически перестраивается на другой управляющий сервер, адрес которого вычисляется в соответствии с определенным алгоритмом. Известно, что Kraken создавали для рассылки спама (до 500 тыс. писем в сутки), но наличие средств обновления бинарного кода не исключает возможности использования ботнета для других задач, таких как совершение DDoS-атак.

Согласно исследованию, проведенному разработчиком антиспамовского программного обеспечения Marshal, 85% от всего объема спама рассылается с помощью шести крупнейших ботнетов. Из них 60% спама приходится на ботнеты Srizbi (генерирует 39% спама) и Rustock (21%).

Примечательно, что самый известный ботнет Storm разослал всего лишь 2%. Червь Storm впервые всплыл еще в 2007-м. За неделю он заразил более полутора миллионов компьютеров по всему миру, пользуясь уязвимостью ОС Windows. Название Storm получено этим червем потому, что первоначально он рассылался электронными письмами с заголовком «230 dead as storm batters Europe». Хотя Storm называют «червем» (эта программа распространяется методом, характерным для почтовых червей), Storm Worm имеет функции трояна/бэкдора, а также может играть роль DDoS-бота — программы, используемой для проведения DDoS-атак. Главной проблемой, связанной с Storm, является сеть зараженных компьютеров — ботнет, включающий несколько десятков миллионов компьютеров. Ботнет Storm ведет себя, как колония муравьев, — с четким распределением ролей между машинами. Узлы сети делятся на распространителей, «командные центры» и «рабочие» компьютеры, которые в обычном режиме просто исполняют приказы, но при необходимости могут брать на себя функции деактивированных «командных центров» или распространителей.

Общеизвестно, что ботнет широко используется для шантажа владельцев онлайн-бизнеса. Известен случай, когда фирма-разработчик инструмента активного противодействия спам-рассылкам была вынуждена уйти из бизнеса ввиду осуществления угрозы DDoS-атаки со стороны разработчиков ботнета.

Рецепты защиты от ботнетов

Как же можно бороться с ботнетами, как защитить корпоративную сеть или отдельные компьютеры, как интернет-провайдерам уберечь компьютеры своих абонентов? Объемы ботнет-ресурсов, названные В. Серфом, опровергают распространенное заблуждение, будто антивирусные программы, устанавливаемые на компьютерах пользователей, га-

Бизнес против бизнеса, или игры без правил в интернет-пространстве

Анна Зарахович, директор Представительства «Тренд Майкро» в Украине и Молдове

— Киберпреступность является на сегодняшний день одной из наиболее актуальных проблем в мире. Стремительное развитие бот-сетей и, соответственно, увеличение количества DDoS-атак связано с тем, что этот вид нелегального бизнеса становится все более популярным в силу своей эффективности и высокой доходности. Эпоха вирусных эпидемий подошла к концу, и сегодня пользователи Интернета все чаще сталкиваются с точечными, «адресными» атаками, и бот-сети служат отличным инструментом для их реализации.

Жертвой «ддосеров» может стать любая компания, на которую поступил «заказ», независимо от сферы и масштабов ее деятельности. Наиболее уязвимы те, чей бизнес хоть каким-либо образом осуществляется через Интернет — интернет-магазины, платежные системы, интернет-казино, интернет-процессинги и т.д. Именно они и составляют основную целевую аудиторию для атакующих.

Проблема бот-сетей, как источника распространения вирусов, спама и инструмента для DDoS-атак, актуальна в Украине ни чуть не менее, чем в мировом пространстве. С точки зрения государственного регулирования, ответственность за информационную безопасность в Украине возложена на Государственную службу специальной связи и защиты информации Украины, деятельность которой регламентируется Законом Украины «О Государственной службе специальной связи и защиты информации Украины». К сожалению, официальные источники не предоставляют в открытом виде для широкой общественности информацию о количестве и, так сказать, «качестве» осуществленных атак на украинских пользователей. Но очевидно, что такая статистика имеется, поскольку Украина, как ни печально, является частью мировой индустрии киберпреступности. При любых атаках на государственные органы сразу реагирует Служба безопасности Украины и проводит соответствующее расследование.

Так, в частности, по данным компании Trend Micro, в Украине генерируется порядка 1,7% мирового объема спама. Лидерами среди государств, рассылающих спам, являются Российская Федерация (10,16%) и США (9,74%). (Более подробная информация содержится на странице http://itw.trendmicro-europe.com/index.php?id=25.)

Небезынтересной является также статистика Trend Micro Threat Recourse Center, отражающая количество ежедневно анализируемых веб-сайтов на предмет наличия вредоносного кода и количество заблокированных ссылок, а также доля источников спама в общем объеме анализируемого почтового трафика. Так, по состоянию на сегодня, свыше 55% всего e-mail трафика блокируется еще на этапе приема почты — благодаря службам почтовой репутации (email reputation service). (Более подробно см. http://itw.trendmicro-europe.com/index.php?id=68.)

Наличие программных и аппаратных средств защиты значительно затрудняет осуществление атаки. Среди решений компании Trend Micro для защиты от вредоносного кода используются службы репутации — Web Reputation Service, E-mail Reputation Service. Эти сервисы не допускают соединение с неблагонадежными серверами (превентивный способ защиты) вне зависимости от того, какая атака идет от бот-сетей (вирусы, спам, DDoS) и тем самым повышают безопасность работы в Интернете.

рантированно могут их защитить и от заражения ботнет-червями. Защита от ботнетов — проблема многоуровневая, требующая комплексных решений.

Следует отметить, что одни лишь специализированные средства не в состоянии противодействовать ботнетам, а должны интегрироваться в общую систему информационной безопасности. Так, основные методы обнаружения «троянских коней» и червей в общем традиционны — проверка сигнатуры кода, эвристический анализ, фиксация подозрительного поведения программ. Антивирусные программы, конечно, могут помочь, но не все и не от всех ботнетов. Для защиты от массовой рассылки спама или вирусов используются промышленные системы защиты от вредоносного кода и нежелательной почтовой корреспонденции. Для противодействия проведению распределенных DDoS-атак используются специализированные программно-аппаратные комплексы. Подобные решения сегодня предоставляют многие производители коммуникационного оборудования и программных средств, например, известны такие системы, как Cisco Guard или межсетевой экран Outpost Firewall Pro. Для защиты от rootkit-технологий (сокрытия присутствия вредоносного программного обеспечения) создаются специальные решения, такие, к примеру, как RootkitRevealer, F-Secure BlackLight Rootkit Eliminator, System Virginity Verifier, AVZ и Safe›n›Sec Rootkit Detector.

В дополнение к стандартным средствам защиты также могут использоваться специализированные сервисы, наподобие ZombieAlert компании Sophos. В его рамках администратор корпоративной сети может получить уведомления в том случае, если будет зафиксировано, что с IP-адресов его сети осуществляется DDoS-атака и выполняется рассылка спама или вирусов. Для обнаружения ботнетов также используют «приманки» (honneypot). Это замкнутая, защищенная и контролируемая область, имитирующая уязвимую сеть или ресурс. Ее основная цель — приманить и обнаружить попытки вторжения, заражения вирусами на ранних стадиях развития атак, используя методы активного анализа.

Создание и использование ботнетов запрещено законодательством многих стран, однако уголовное преследование авторов и владельцев ботнетов — чрезвычайно редкое событие. Пока можно привести лишь два случая, когда авторы ботнетов понесли реальное наказание. Так, двадцатилетний американец Дж. Антаче, создавший ботнет, который заразил 400 тысяч компьютеров, в том числе на авиабазах ВМС США в Чайна-Лейк, получил срок заключения в 57 месяцев и оштрафован на 75 тыс. долларов. Известен еще

один приговор, вынесенный в Нидерландах, когда заразившие несколько миллионов компьютеров злоумышленики были оштрафованы в общей сложности на 13 тыс. евро.

Проводя в жизнь акцию «Operation Bot Roast», американские власти объявили войну ботнетам, этой «растущей угрозе национальной безопасности, национальной информационной инфраструктуре и экономике». В настоящее время многие компании и организации ФБР совместно со специалистами по компьютерной безопасности, включая Координационный центр CERT при университете Карнеги-Меллон, разрабатывают систему оповещения владельцев зомби-компьютеров из ботнетов о захвате контроля над их машинами, сбора и обработки свидетельств криминальной активности с зараженных машин и восстановления нормальной работоспособности последних. То есть защитники информации и борцы с ботнетами без дела не останутся. Подразделениям информационной безопасности приходится постоянно заботиться о предотвращении заражения компьютеров и защите информационных ресурсов от атак, проводимых ботнетами.

Из приведенных выше фактов следует, что в настоящее время ботнеты являются основной угрозой безопасности в Интернете. Ботнеты динамичны, распределены, а значит, их сложно обнаружить и обезвредить. Вред, наносимый ботнетами, огромен, а наказания за создание и использование — ничтожны.

Дмитрий ЛАНДЭ, *д.т.н., зам. директора ИЦ ElVist*