направлений подготовки 230700 «Прикладная информатика», 080500 «Бизнес-информатика», системы профессиональной подготовки и повышения квалификации). Поданы документы на получение свидетельства ОФАП об отраслевой регистрации ЭУМК «Информационная безопасность в открытом образовании». Исполнителями проекта написана монография «Аудит информационной инфраструктуры компании и разработка ИТ-стратегии» (О.Б. Назарова, Л.З. Давлеткиреева и др.). По результатам проекта опубликовано 18 публикаций, из них 12 статей (в том числе 1 из реестра ВАК), 4 тезисов, 1 сборник научных трудов, 1 монография, 2 ЭУМК.

Библиографический список

1. *Чусавитина Г.Н. , Чусавитин М.О.* Подготовка студентов педагогических специальностей университета к профилактике и противодействию идеологии киберэкстремизма среди молодежи, II Всероссийская научно-практическая конференция «Информационные технологии в образовании XXI века». //Сборник научных трудов. Т. 1. – М.: НИЯУ МИФИ.2012 -376с., Москва, 2012, -С. 322 – 326.

2. *Чусавитина Г.Н. , Чусавитин М.О.* Модель подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде// Материалы Международной научно-практической конференции «Новые информационные технологии в образовании», ФГАОУ ВПО «Рос. гос. проф.-пед. ун-т»., Екатеринбург, 2012, -С.519 – 521.

Е.Д. Шамонин

УГРОЗЫ, ИСХОЯЩИЕ ОТ ЗОМБИ-СЕТЕЙ

shamonined@mail.ru

Институт математики и компьютерных наук УрФУ, г. Екатерибург

Оснащение учебных заведений огромным количеством средств вычислительной техники (СВТ), в том числе с возможностью выхода в глобальную сеть Интернет, кроме беспрецедентных возможностей по автоматизации процессов обучения влечет за собой и ряд весьма негативных факторов, наиболее грозным из которых является вовлечение части этих компьютеров в зомби-сети (ботнеты).

Хотя термин «ботнет» может обозначать любую группу ботов, например IRC (Internet Relay Chat) ботов, обычно его относят к группе компьютеров, зараженной специальной программой — сетевым червем или троянской программой, управляемой из одного источника. Владелец ботнета может удаленно управлять группой, обычно через IRC сервер или специальный канал в публичной IRC сети. Заражение систем осуществляется с использованием различных инструментов (эксплойты, переполнение буфера и др.). Новые боты — компьютеры, вовлеченные в зомби-сети — могут автоматически сканировать среду, обнаруживать уязвимости, осуществлять атаки на слабые пароли, производить рассылку спама и пр. Ботнеты обладают мощными вычислительными ресурсами, являются грозным кибероружием и хорошим способом зарабатывания денег для злоумышленников.

Управление компьютером, который заражен ботом, может быть прямым и опосредованным. В случае прямого управления злоумышленник может установить связь с инфицированным компьютером и управлять им, используя встроенные в тело программы-бота команды. В случае опосредованного управления бот сам соединяется с центром управления или другими машинами в сети, посылает запрос и выполняет полученную команду.

В любом случае хозяин зараженной машины, как правило, даже не подозревает о том, что она используется злоумышленниками. Именно поэтому зараженные вредоносной программой-ботом компьютеры, находящиеся под тайным контролем киберпреступников, называют еще зомби-компьютерами, а сеть, в которую они входят — зомби-сетью.

На сегодняшний день ботнеты являются одним из основных источников нелегального заработка в Интернете и грозным оружием в руках злоумышленников. Ожидать, что киберпреступники откажутся от столь эффективного инструмента, не приходится, и эксперты по безопасности с тревогой смотрят в будущее, ожидая дальнейшего развития ботнет-технологий. На сегодняшний день основными направлениями использования зомби-сетей являются следующие.

Рассылка спама. Это наиболее распространенный и один из самых простых вариантов эксплуатации ботнетов. По экспертным оценкам, в настоящее время более 80% спама рассылается с зомби-машин. Спам с ботнетов не обязательно рассылается владельцами сети. За определенную плату спамеры могут взять ботнет в аренду.

Кибершантаж. Ботнеты широко используются и для проведения DDoS атак (Distributed Denial of Service — распределенная атака типа «отказ в обслуживании»). В ходе такой атаки с зараженных ботом машин создается поток ложных запросов на атакуемый сервер в Сети. В результате сервер из-за перегрузки становится недоступным для пользователей. За остановку атаки злоумышленники, как правило, требуют выкуп.

DDoS-атаки могут использоваться и как средство политического воздействия. В этих случаях атакуются, как правило, серверы государственных учреждений или правительственных организаций. Опасность такого рода атак состоит еще и в том, что они могут носить провокационный характер: кибератака серверов одной страны может осуществляться с серверов другой, а управляться с территории третьего государства.

Анонимный доступ в Сеть. Злоумышленники могут обращаться к серверам в Сети, используя зомби-машины, и от имени зараженных машин совершать киберпреступления — например, взламывать веб-сайты или переводить украденные денежные средства.

Фишинг — получение данных по кредитным картам, банковским счетам с использованием поддельных сайтов. Адреса фишинговых страниц могут довольно быстро попасть в черные списки («время жизни» до 5 дней). Ботнет дает возможность фишерам быстро менять адрес фишинговой страницы, используя зараженные компьютеры в роли прокси-серверов. Это позволяет скрыть реальный адрес веб-сервера фишера.

Кража конфиденциальных данных. Этот вид криминальной деятельности, пожалуй, никогда не перестанет привлекать киберпреступников, а с помощью ботнетов улов в виде различных паролей (для доступа к E-Mail, ICQ, FTP-ресурсам, веб-сервисам) и прочих конфиденциальных данных пользователей увеличивается в тысячи раз. Бот, которым заражены компьютеры в зомби-сети, может скачать другую вредоносную программу – например, троянскую программу, ворующую пароли. В таком случае инфицированными троянской программой окажутся все компьютеры, входящие в эту зомби-сеть, и злоумышленники смогут заполучить пароли со всех зараженных машин. Украденные пароли перепродаются или используются, в частности, для массового заражения веб-страниц (например, пароли для всех найденных FTP-аккаунтов) с целью дальнейшего распространения вредоносной программы-бота и расширения зомби-сети.

Опасность ботнетов усугубляется тем, что их создание и использование становится все более простой задачей, с которой в ближайшем будущем будут в состоянии справиться даже школьники. А цены на развитом и структурированном ботнет-рынке весьма умеренные.

В построении интернациональных ботнетов могут быть заинтересованы не только киберпреступники, но и государства, готовые использовать зомби-сети как инструмент политического давления. Кроме того, возможность анонимно управлять зараженными машинами вне зависимости от их географического нахождения позволяет провоцировать конфликты между государствами: достаточно организовать кибератаку на серверы одной страны с компьютеров другой.

Сети, объединяющие ресурсы десятков, сотен тысяч, а порой и миллионов зараженных машин, обладают очень опасным потенциалом, который пока не использовался в полном объеме.