С.В. Середа
Криворожский государственный
педагогический университет
IV курс, группа И-05
Научный руководитель:
к.пед.н., доц. С.А. Семериков

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ МОДЕЛИРОВАНИЯ БОТ-СЕТЕЙ

Ботнет (англ. botnet) – это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами – автономным программным обеспечением. Чаще всего бот в составе ботнета является скрытно устанавливаемым на компьютере жертвы и позволяющим злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера программным обеспечением. Обычно используются для нелегальной или неодобряемой деятельности – рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании, но так же может применяться и в благих целях, например, распределенные вычисления.

Управление обычно получают в результате установки на компьютер специального программного обеспечения. Управление производится или «слушанием» определённой команды по определённому порту, или присутствием в IRC-чате. До момента использования программа находится в режиме ожидания. По получению команды от «владельца» ботнета, начинает исполнять команду (один из видов деятельности). В ряде случаев по команде загружается исполняемый код (таким образом, имеется возможность

«обновлять» программу и загружать модули с произвольной функциональностью). В настоящее время получили распространение ботнеты управляемые через веб-сайт или по принципу p2p-сетей.

На рис. 1 изображена централизованная модель ботнета – самая популярная модель в плане реализации ботнетов, легко реализовывается на базе одного центрального сервера к которому подключаются RAT. Примером может быть просто веб-сервер, к которому подключаются RAT. Далее они получают команды, которые находятся на веб-сервере.

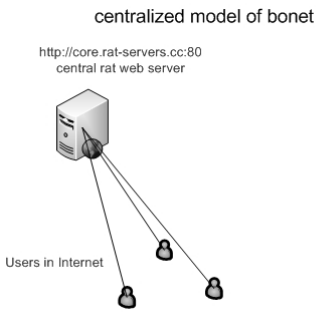

Рис. 1

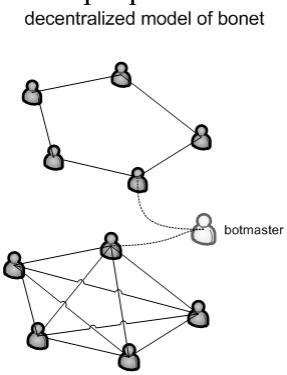

Рис. 2

Децентрализованная модель (рис. 2) – одна из самых сложных систем в плане реализации, суть заключается в том ,что каждый RAT поддерживает соединение с другой RAT, у этой системы отсутствует центральный сервер, который бы командовал. Для этого придется подключаться к одному из узлов сети и отсылать команды по цепочке всем RAT. Сложная система востребована только в небольших сетях.

Распространено мнение, что, по крайней мере, каждый второй домашний компьютер, подключенный к Интернету, состоит сегодня в какой-либо бот-

сети. Это не означает, что бот-сеть обязательно действующая: многие сети могут находиться в «ждущем режиме». Но факт – остается фактом – машина заражена и подобно «спящему вулкану» таит в себе потенциальную как для своего владельца, так и для других машин в сети. Угроза распространения зомби-сетей постоянно растет. Количество разновидностей бот-вирусов только в 2005 году увеличилось на 538%.

Противодействовать такому массовому распространению бот-сетей крайне сложно. Крупную сеть из «компьютеров-зомби» можно сделать за неделю-две. А на ее обнаружение и нейтрализацию могут потребоваться месяцы работы. Выйти же на владельца бот-сети – еще более трудновыполнимая задача.