UDC 004.491.2

VIRAL NETWORK BOTNET

[1] Yuri D. Ivasyuk
[2] Ivan A. Doluev

[1] Sochi State University for Tourism and Recreation
Sovetskaya street 26a, Sochi city, Krasnodar Krai, 354000, Russia
PhD (technical), Assistant of professor
[2] Sochi State University for Tourism and Recreation
Sovetskaya street 26a, Sochi city, Krasnodar Krai, 354000, Russia
Student
E-mail: Juriji@mail.ru

The article discusses the new technology of computer viruses-"spies". These viruses (bots) form the control of computer networks, called botnets.

Keywords: hacker, program-"spies", computer network, host, technology "stels", spam, firewall.

14 апреля 2011 года в на сайте Газета.ру появилась интересная статья о том, как российские хакеры «заражают» США. Выдержка из статьи: «Правоохранительным органам США удалось раскрыть одну из крупнейших хакерских схем. По данным министерства юстиции США, с помощью вируса Coreflood была создана сеть из 2 млн зараженных компьютеров, так называемый ботнет. С ее помощью хакеры воровали по всему миру личные данные пользователей и сведения об их кредитных картах. Объем похищенных средств мог достигать $100 млн». Управление сетью осуществлялось через трояны. Эти программы - "шпионы" отслеживали работу пользователей на клавиатуре и мыши. И, наконец, stels-технологии обеспечивали ботнету анонимность и незаметность.

В современном обществе владение информацией дает значительные преимущества в конкурентной борьбе. Одна из целей зомбирования (установка бот-программы на хост) – получение информации о пользователе: его адрес, телефон, фамилию, имя, номера кредитных карт, логинов и паролей, вплоть до адресов электронной почты его друзей и знакомых, а так же для организации хакерских атак. Что же такое «ботнет»?

Ботнет (англ. *botnet* от robot и network) – это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами – автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на компьютере жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера. Ботнет состоит из:

1) "Бот-компьютер" – это компьютер, на котором установлена бот программа, при помощи которой, "хозяин" может управлять этим компьютером.

2) "Бот-программа" – это программа, которая выполняет какое-то определённое действие автоматически (для которого она была создана), и которой в большинстве случаев дистанционно управляет её "хозяин". Боты могут быть разными, бывают ICQ боты, бывают боты, которые предназначены для спама сайтов, боты которые «сидят» на сайтах, чатах, автоматически отравляя сообщения или отвечая на них.

Зараженный компьютер, бот-программа превращает в так называемый "Компьютер-зомби" который подчиняется своему "хозяину". Ботнеты чаще всего используются хакерами для рассылки спама с этих зараженных компьютеров, так же их используют в качестве системы прокси, при этом хакер остаётся незамеченным, совершая взломы. Ботнеты также используют для DDos атак, что заключается в посылке множество пакетов разной информации на атакуемый сервер с зараженных компьютеров, что приводит к тому, что атакуемый сервер тратит все свои ресурсы на обработку этих запросов, а на запросы обычных пользователей уже ответить не может, и сервер «виснет». Но для этого нужна уже большая сеть зараженных компьютеров. Многие боты используют так называемую технологию "stels", которая позволяет боту быть полностью невидимым в системе, и сидеть там так тихо, что пользователь даже не будет и подозревать, что в его системе находиться бот. Некоторые боты-черви используют технологию самораспространения. Используя нашумевшие дыры в ОС Windows, боты могут сами распространяться по сети, заражая ежедневно сотни
и тысячи компьютеров.

Защита от этой «напасти» есть, и она очень похожа на защиту от вирусов в интернете – хороший файрвол или антивирус (либо их сочетание). Однако, как показывает опыт, всякую защиту можно обойти. Если Skype умеет обманывать файрвол, то почему это не может сделать бот-программа? Для того чтобы это не произошло необходимо упаковать антивирус/файрвол достойным протектором, препятствующим сигнатурному поиску и внедрению в охраняемый процесс постороннего кода. Эта простая защита позволяет защитить файрвол от самых сложных атак и даёт высокую вероятность того, что ваш компьютер не попадёт в ботнет.

УДК 004.491.2

ВИРУСНАЯ СЕТЬ БОТНЕТ

[1] Юрий Дмитриевич Ивасюк
[2] Иван Александрович Долуев

[1] Сочинский государственный университет туризма и курортного дела
354000, Россия, Краснодарский край, г. Сочи, ул. Советская, 26 а
Кандидат технических наук, доцент
E-mail: Juriji@mail.ru
[2] Сочинский государственный университет туризма и курортного дела
354000, Россия, Краснодарский край, г. Сочи, ул. Советская, 26 а
Студент

В статье рассматривается новая технология использования компьютерных вирусов – «шпионов». Эти вирусы (боты) формируют управляемые ими компьютерные сети, так называемые ботнеты.

Ключевые слова: хакер, программы-"шпионы", компьютерная сеть, хост, технология "stels", спам, файрвол.