Метод обнаружения ботнетов на основе многоагентного подхода

М.Ю. Косенко
Институт информационных технологий
Челябинский государственный университет
Челябинск, Россия
e-mail: kosenko@csu.ru

Аннотация[1]

В работе представлен метод обнаружения ботнетов на основе многоагентного подхода. Данный метод основывается на работе распределенной системы обнаружения и блокирования атак типа «отказ в обслуживании» с последующим определением признаков атакующего бота и выявлением по этим признакам участников ботнета в сети Интернет.

1. Введение

Одной из самых опасных угроз безопасности в сети Интернет являются ботнеты. Ботнет – это компьютерная сеть, состоящая из скомпрометированных хостов управляемых некоторым вредоносным программным обеспечением (бот). Бот является частично автономной частью вредоносного программного обеспечения, которое контролируется удаленно. Ботнеты создаются путем инфицирования компьютера без ведома и согласия его владельца, например, рассылка вирусов прикрепленных к электронным письмам [1]. Применяются подобные сети для множества зловредных действий: абузоустойчивый хостинг (размещение порнографического, террористического контента), проведение атак типа «отказ в обслуживании», заражение шпионским вредоносным программным обеспечением, хищение конфиденциальных данных, широкомасштабная рассылка спама, «накручивание» кликов.

В настоящее время злоумышленниками отработаны техники построения ботнетов. Примеры известных зараженных сетей [2]:

- Ботнет Bredolab. Состоял примерно из 30 миллионов компьютеров. Использовался для организации DDOS-атак (в том числе на ряд российских новостных ресурсов, на сайт «Лаборатории Ксаперского»). В 2010 году принес своему создателю прибыль в размере 700 тысяч долларов. Методы распространения: эксплойт-пак, модификация страниц сайтов с ссылками на вредоносное программное обеспечение;
- Ботнет Storm. Использовался для рассылки спама, организации DDOS-атак. Около 2 миллионов зараженных компьютеров. Распространялся путем почтовых рассылок.
- Ботнет Spyeye. Использовался для банковского мошенничества. Состоял из 1,4 миллиона компьютеров.
- Ботнет Mariposa. Использовался для кражи конфиденциальной информации, организации DDOS-атак. Состоял из 12 миллионов компьютеров.
- Ботнет Zeroaccess. Использовался для «накручивания» кликов, рассылки спама, добывания bitcoin. Состоял примерно их 9 миллионов компьютеров;
- Ботнет Zeus. Использовался для банковского мошенничества. Состоял примерно из 13 миллионов компьютеров;
- А также, DDOS-ботнет DRAGON, спам-ботнет Grum (около 1 млн. инфицированных компьютеров, 18 млрд. писем в месяц на пике работы), спам-ботнет Virut (более 300000 зараженных устройств) [3].

Такое многообразие различных ботнетов показывает, что создание и использование ботнетов – это одно из наиболее популярных направлений кибер-преступности. Таким образом, одной из актуальных задач на сегодняшний день становится задача идентификации участников ботнетов.

К наиболее распространенным методам обнаружения ботнетов относится:

Анализ телеметрии. Метод заключается в использовании сводной информации сетевого и транспортного уровня от сетевых устройств. К примеру, технология NetFlow часто применяется для обнаружения трафика DDOS атак, всплесков трафика SMTP, характерного для массовой рассылки спама и управляющего трафика контроллера ботнета.

Труды второй международной конференции "Интеллектуальные технологии обработки информации и управления", 10 - 12 ноября, Уфа, Россия, 2014

Обнаружение аномалий. В отличии от подхода на основе сигнатур, заключающегося в сопоставлении каждой атаки с имеющейся базой данных сигнатур, обнаружение аномалий заключается в обратном: описываются характеристики обычного трафика, а затем выполняется поиск отклонений. Использование такого подхода обеспечивает обнаружение и блокировку DDOS атак и попыток массового сканирования, предпринимаемых ботнетами.

Анализ журнала сервера DNS. Ботнеты часто используют бесплатные службы DNS, чтобы разместить адрес поддомена управляющих серверов, от которых можно принимать команды управления и получать обновления вредоносного кода. Часто код бота содержит жестко заданные ссылки на DNS-сервер, которые могут быть легко найдены любым средством анализа журнала DNS-запросов. При обнаружении таких служб администратор DNS-сервера может нейтрализовать ботнет путем переадресации зловредных поддоменов на несуществующий IP-адрес.

Система Honeypot. Ресурс-приманка, представляемый замкнутую, защищенную и контролируемую область, имитирующую уязвимую сеть, ресурс или сервис. Основная цель – приманить и обнаружить вредоносные атаки и попытки вторжения.

В различных методах встречаются проблемы при их масштабировании, либо в вопросах автоматизации процесса обнаружения ботнета.

2. Метод идентификации участников ботнетов.

Целью данной работы является описание метода идентификации участников ботнетов на основе многоагентного подхода. Многоагентный подход фактически избавляет от проблем масштабирования при росте системы идентификации. Выявление набора одинаковых признаков взаимодействия ботов с контролерами ботнетов могут решить проблему автоматизации обнаружения ботов. Таким образом необходимо решить следующие задачи:

1. Выделить набор признаков по которым возможно осуществлять идентификацию ботов.
2. Построить архитектуру многоагентной системы идентификации ботов.
3. Разработать модель интеллектуального агента.

В качестве общих признаков ботов можно выделить:

- IP-адрес или доменное имя контролирующего центра ботнета;
- характеристики HTTP или IRC пакетов с определенными командами управления;
- размерность сетевых пакетов;
- временные интервалы сетевых взаимодействий;
- трафик злонамеренной активности, к примеру, сканирование, рассылка спама, загрузка бинарных файлов [4, 5];
- информацию протоколов DNS, SMTP;
- используемый протокол обмена данными и порты транспортного уровня.

Многоагентная архитектура системы идентификации ботов базируется на средстве защиты от распределенных атак типа «отказ в обслуживании» с возможностью обнаружения атаки в сети цели атаки, а предотвращения генерации атаки в сети источника. Концептуальная схема такой системы приведена на Рисунке 1. Архитектура многоагентной системы идентификации ботов состоит из следующих элементов:

1. Аналитический модуль. Модуль, устанавливаемый в каждой автономной системе сети Интернет, состоящий из подсистемы обнаружения атаки (аналитический модуль DDOS) и подсистемы выявления признаков ботнета (аналитический модуль botnet). Каждая подсистема анализирует сетевой трафик, одна с целью обнаружения атак типа «отказ в обслуживании», другая с целью определить признаки ботнета.
2. Модуль реагирования на обнаруженные атаки. Устанавливается в любой точке глобальной сети Интернет. Предназначен для централизованной передачи команд управления модулям блокировки атак и агентам идентификации ботнетов. Помимо прочего, осуществляет отсылку уведомления об атаке, либо обнаружении ботнета в модуль визуализации.
3. Модуль блокирования атаки. Устанавливается в сети источника атаки. Осуществляет реагирование на основе информации полученной от модуля реагирования согласно профилю сетевой безопасности (блокирование систем задействованных в реализации атаки, оповещение ответственных лиц по электронной почте, SMS).
4. Агент идентификации ботнета. Анализирует траффик сети на наличие признаков функционирования ботов. При обнаружении бота агент оповещает модуль реагирования.
5. Модуль визуализации атак. Может работать в рамках сервера реагирования. Предназначен для предоставления графического интерфейса визуализации обнаруженных атак.
6. Модуль хранения. Может работать в рамках сервера реагирования, модуль основан на системе управления базами данных. Позволяет хранить и обеспечивать доступ к истории обнаруженных атак.

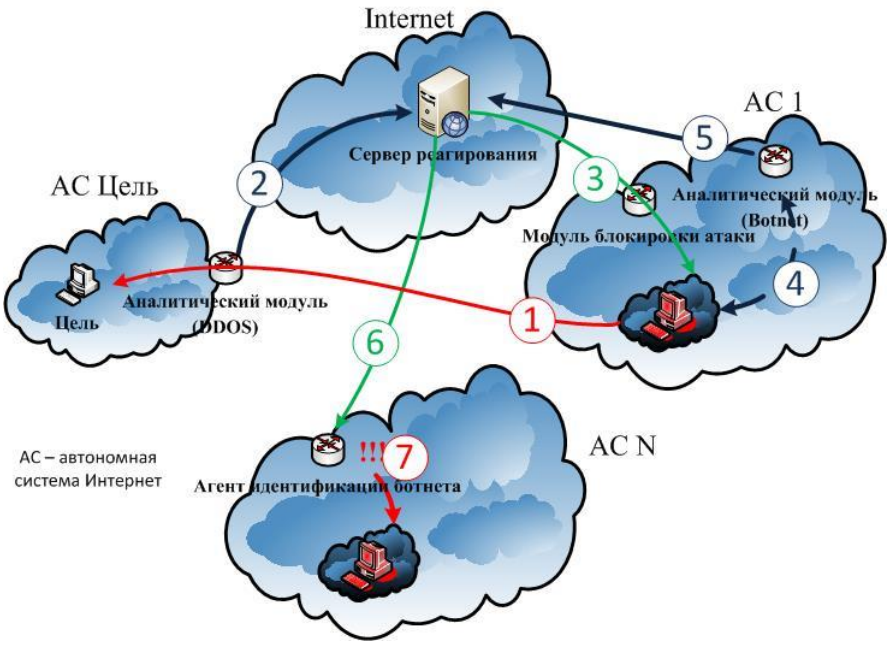

Рис. 1. Схема многоагентной системы идентификации ботнетов.

Концептуальный алгоритм функционирования системы заключается в следующем:

1. Аналитический модуль (DDOS) при обнаружении атаки типа «отказ в обслуживании» передает информацию о ней модулю реагирования.
2. Модуль реагирования передает в модуля блокирования атаки, находящихся в соответствующих источникам атаки автономных системах, команды блокирования атаки. А так же, дает указание аналитическому модулю (botnet) начать анализ систем участвующих в обнаруженной атаке.
3. Аналитический модуль (botnet) выявляет характерные признаки ботнета, участники которого производили атаку и передает эти признаки модулю реагирования.
4. Модуль реагирования рассылает признаки ботнета всем агентам идентификации ботнета.
5. Агенты идентификации ботнета анализируют трафик в своей сети, пробуя обнаружить полученные признаки работы ботнета. В случае удачной идентификации, передают информацию о боте в модуль реагирования для дальнейшего принятия решения.

3. Заключение

Предложенный метод позволяет обнаружить ботнетов на основе анализа функционирования ботов участвующих в конкретной атаке. Особенность метода заключается в возможности идентифицировать ботов не принимавших участия в атаке за счёт работы распределенной сети интеллектуальных агентов. В работе предложено:

- архитектура многоагентной системы идентификации ботнетов;
- концептуальный алгоритм работы подобной системы.

Направлениями дальнейших исследований автора являются:

- разработка модели интеллектуального агента;
- разработка метода анализа агентами траффика автономной системы;
- оценка эффективности предложенной модели и метода анализа, используя разработанные программные решения.

Список используемых источников

1. Ianelli, N. and Hackworth, A. «Botnets as a vehicle for online crime.» CERT Coordination Center, 2005, pp 1-28.
2. Трегубенко В., «Топ-10 ботнетов», Хакер №188, 2014.
3. Group-IB Threat Intelligence Report 2012 – 2013 H1.
4. Zhuge J., Holz T., Han X., Guo J., Zou W., "Characterizing the ircbased Botnet phenomenon." Peking University& University of Mannheim Technical Report, 2007.
5. Collins M., Shimeall T., Faber S., Janies J.,Weaver R, Shon M.D., Kadane J., "Using uncleanliness to predict future Botnet addresses" in Proceedings of ACMIUSENIX Internet Measurement Conference (IMC'07),2007.