ВОПРОСЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ БОТНЕТ АТАК

Косенко М.Ю.[1], Мельников А.В.[2]

Вредоносное программное обеспечение, автономно и автоматически работающее на зараженных компьютерах, образующих ботнеты, используется как основная платформа для совершения распределенных атак на различные информационные системы. Используя ботнеты реализуют различную криминальную деятельность: распределенные атаки типа «отказ в обслуживании», рассылка спама, фишинг, кликфрод, кража информации, распространение других нежелательных программ, абузоустойчивый хостинг. Традиционные техники обнаружения вторжений и вредоносного программного обеспечения полезны для обнаружения определенных признаков ботнетов, но как таковые, не ориентированы на осуществление эффективной борьбой с ними. В статье рассматриваются шесть этапов жизненного цикла ботнетов и показано, что ботнет можно рассматривать как многоагентную систему. Проанализированы различные методы защиты от ботнетов, приведены преимущества и недостатки данных методов. Предложена многоагентная система обнаружения и блокирования ботнетов, приведена структура данной системы и предложена схема развертывания прототипа системы. Обоснован подход обнаружения ботнета на этапах взаимодействия и выполнения атаки, с учётом жизненного цикла ботнета.

***Ключевые слова**: обнаружение ботнетов, средство защиты от ботнетов, жизненный цикл ботнетов, многоагентная система защиты, система обнаружения вторжений*

DOI 10.21681/2311-3456-2016-4-20-28

Введение

Большинство атак и мошеннических действий в Интернете осуществляется с помощью вредоносного программного обеспечения, которое включает в себя вирусы, трояны, черви, шпионские программы, а также и ботнеты. Вредоносное программное обеспечение стало основным источником большинства вредоносной активности в Интернете: целевые атаки [1], распределенные атаки типа «отказ в обслуживании», мошеннические действия [2], а также сканирование. Среди всех видов вредоносного программного обеспечения, ботнеты являются основной платформой [2], которую злоумышленники используют как масштабный, согласованно действующий инструмент, используемый для поддержки постоянного роста преступной деятельности, такой как DDoS, рассылка спама, фишинг и кража информации.

Жизненный цикл ботнетов

Бот – это программное обеспечение робота, экземпляр вредоносного программного обеспечения, работающий на зараженном компьютере автономно и автоматически без ведома пользователя. Код бота, как правило, профессионально написан финансируемыми преступными группами и содержит обширный набор функциональных возможностей, чтобы иметь возможность выполнять множество вредоносных действий. В некоторых случаях под термином «бот» подразумевается инфицированный ботом компьютер. Ботнет – это сеть ботов, которые находятся под удаленным контролем злоумышленника. Злоумышленника, контролирующего ботнет называют бот-мастером. Бот-мастер управляет ботнетом посредством некоторых каналов команд и управления (Command and Control, C&C).

В настоящее время ботнеты являются одной из основных причин криминальной деятельности в Интернете [3], такой как:

• Распределенные атаки типа «отказ в обслуживании» (Distributed Denial of Service, DDOS). Ботнету может быть отдана команда совершить целенаправленную, распределенную атаку типа «отказ в обслуживании» на любую систему в Интернете с целью поглотить ресурсы (например, пропускная способность) системы таким образом, что она не сможет должным образом обслуживать своих легитимных пользователей. В настоящее время практически все DDoS-атаки осуществляются с платформы ботнетов. Несмотря на простоту техники атаки DDoS, она является очень эффективной за счет размеров ботнета и общей пропускной способности ботов. К примеру, одна из самых известных за последнее время, это DDoS

1 Косенко Максим Юрьевич, Челябинский государственный университет, Челябинск, kosenko@csu.ru

2 Мельников Андрей Витальевич, доктор технических наук, профессор, Челябинский государственный университет, Челябинск, mav@csu.ru

атака против популярного веб хостинга ИТ проектов GitHub в марте 2015 года [4].

• Рассылка спама. Более 95% электронной почты в сети Интернет является спамом, что составляет несколько миллиардов сообщений спама в интернет трафике ежедневно. Большинство этих сообщений спама, на самом деле, отправлены из ботнетов. Точный процент спама исходящий от ботнетов может варьироваться в зависимости от различных статистических данных, многие люди считают, что в настоящее время этот процент составляет более 95%. Ряд известных ботнетов были использованы для рассылки спама, в том числе Bobax, ранний спам бот использующий HTTP в качестве C&C, и Storm Worm (он же Peacomm), еще один печально известный P2P ботнет агрессивно проводящий рассылку спама.

• Фишинг. Ботнеты широко используются для размещения вредоносных поддельных сайтов. Обычно преступники рассылают сообщения спама (например, с использованием ботнетов) с целью обманом заманить пользователя посетить поддельные сайты (как правило, связанные с финансовой деятельностью – интернет банкингом). Таким образом, преступники могут получить доступ к конфиденциальной информации пользователей, такой как имена пользователей, пароли и номера кредитных карт. Согласно отчету «Спам и фишинг» компании «Лаборатория Касперского» в третьем квартале 2015 г. с помощью системы «Антифишинг» было предотвращено 36 300 537 попыток перехода пользователей на фишинговые сайты.

• Кликфрод. Ботмастер может получать прибыль от управления кликами ботов на онлайн объявления (то есть посылать HTTP запросы на веб-страницы рекламодателя) с целью личной или коммерческой выгоды. Кликфрод может использоваться для повышения рейтинга веб-сайтов в поисковых системах. Например, ботнет Clickbot.A, использующийся для выполнения малозаметных атак мошеннического клика, симулирует поведение большого числа обычных пользователей.

• Кража информации. Боты активно используются для кражи конфиденциальной информации, такой как номера кредитных карт, пароли или ключи авторизации на локальном компьютере пользователя. Бот может легко украсть пароль от аккаунта дистанционного банковского обслуживания используя кейлоггеры и захват экрана.

• Распространение других нежелательных программ, например, рекламное/шпионское программное обеспечение. Ботнеты являются хорошей платформой для распространения множества других форм вредоносного ПО.

• Абузоустойчивый хостинг. Зараженные компьютеры могут использоваться для размещения на них различного запрещенного контента, например, детской порнографии или террористического материала.

Чтобы глубже понять природу ботнетов, нужно рассмотреть их жизненный цикл. Он, как правило, состоит из нескольких этапов (рис. 1): концепция, распространение, взаимодействие, маркетинг, выполнение атаки, оценка результатов атаки [5], [6]

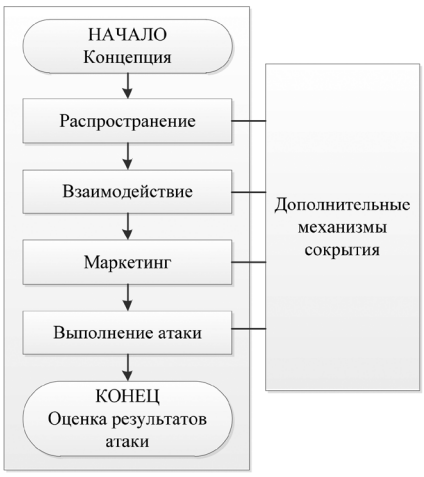

***Рис.1**. Этапы жизненного цикла ботнета*

На первом этапе жизненного цикла любого ботнета определяется его *концепция*. Для создания ботнета существенным элементом является мотивация. Именно от нее будут зависеть архитектура и разработка ботнета. На этой стадии определяются конструктивные характеристики, которые определяются конкретной целью создания ботнета. Этап состоит из двух основных процессов: проектирования и разработки. На этапе проектирования определяется организационная структура ботнета, которая может быть трех типов:

• Централизованная. Все зараженные компьютеры находятся под централизованным управлением, т.е. управляются с помощью выделенного управляющего сервера. Такая структура является наиболее распространенной.

• Децентрализованная. В этом случае, все компьютеры передают команды управления между собой. Структура строится по технологии P2P [7].

• Гибридная. Включает в себя несколько равноправных подсетей бонета, каждая из которых управляется выделенным узлом [8].

Распространение. После того, как вредоносный код бота разработан, необходимо распространить его. Как правило, это достигается за счет

эксплуатирования уязвимостей узлов и внедрения на них ботов. Путей для распространения вредоносного ПО достаточно много. Например, заразить удаленные уязвимые узлы через прямую эксплуатацию уязвимостей, либо распространить через подходы социальной инженерии, таких как электронная почта и мгновенные сообщения. В последнее время бот-мастера используют скомпрометированные веб-сервера, чтобы заразить тех, кто посещает веб-сайты используя технику «попутной загрузки» [9]. При использовании нескольких векторов распространения, бот-мастер может заразить много жертв. В настоящее время ботнет обычно содержит от десятков до сотен тысяч ботов, однако некоторые из них содержат несколько миллионов ботов.

Этап *взаимодействия* описывает взаимодействие между бот-мастером и ботами, и включает в себя два различных процесса. Первый заключается в регистрации скомпрометированного узла в роли функционирующей части ботнета. Второй процесс состоит в обеспечении управляющей связи для ботнета. Бот-мастер должен держать связь с ботами через управляющий канал. Обмен информации состоит из передачи команд от бот-мастера к ботам и операций технического обслуживания (обновление кода, учет членства и т.д.).

Маркетинг. Наиболее распространенной мотивацией для разработчиков ботнета является получение денежной прибыли. С учетом того, что монетизация ботнета может происходить по разному, к примеру, сдача в аренду, либо продажа услуг, разработчику понадобятся клиенты. Чтобы приманить клиентов, разработчик должен опубликовывать информацию о ботнете на приватных форумах, описывать преимущества и возможности своей разработки.

Выполнение атаки. На этом этапе бот-мастер отдает команду ботам выполнить атаку. Ботнет осуществляет вредоносную активность.

Оценка результатов атаки. Конечной целью любого ботнета является возможность успешного выполнения атак. Для контроля реализации цели необходимо проводить этап оценки результатов атаки. Если результат оценки показывает безуспешность функционирования, то ботнет становится бесполезным и все ресурсы, задействованные на предыдущих этапах, становятся потраченными впустую.

Как показано на Рисунке 1 в рамках этапов жизненного цикла ботнета существуют различные дополнительные механизмы. Эти механизмы, как правило, сосредоточенны на скрытии бота от средств защиты. В качестве примеров скрывающих механизмов можно привести: шифрование, обфускация кода, полиморфизм, IP-спуффинг, EMAIL-спуффинг.

Получается, что после выполнения этапа распространения и взаимодействия, бонет представляет из себя множество организационных единиц, управляемых некоторым бот-мастером. Все боты обладают одинаковым функционалом, позволяющим им осуществлять различные атаки на этапе выполнения атаки. Согласно Тарасову В.Б. [10], любая многоагентная система состоит из следующих основных компонентов:

1) множество организационных единиц, в котором выделяются подмножество агентов, манипулирующих подмножеством объектов;
2) множество задач;
3) среда, т.е. некоторое пространство, в котором существуют агенты и объекты;
4) множество отношений между агентами;
5) множество действий агентов.

Таким образом, рассмотрев жизненный цикл бонета, можно заметить, что любой ботнет является многоагентной системой.

Обзор методов защиты от ботнетов

Выделяют различные методы защиты от ботнетов. Основные среди них, это: обнаружение вторжений и вредоносного программного обеспечения, использование сетей приманок.

Обнаружение вторжений и вредоносного программного обеспечения.

Существующие техники обнаружения вторжений [11] и ВПО можно классифицировать на сетевые решения и решения, функционирующие на узлах. Используемые на узлах техники обнаружения очень важны для распознавания исполняемых файлов ВПО и аномалии в поведении на уровне узла. Среди этих методов, антивирусные инструменты полезны для традиционного обнаружения вирусов в течении длительного времени. Другой типичный пример метода обнаружения вторжения на основе узла – это мониторинг системных вызовов.

Когда встает проблема обнаружения ботнетов, эти методы обнаружения, основанные исключительно на анализе узла имеют некоторые проблемы. Во-первых, традиционные антивирусные инструменты основаны на поиске сигнатур, таким образом, требуют объемную, точную и часто обновляемую базу сигнатур. Во-вторых, системы обнаружения на основе узла находятся на том же уровне привилегий, что и боты на некотором узле.

Таким образом, боты могут отключить антивирусные средства системы или использовать руткит-технологии, чтобы защитить себя от обнаружения на локальном узле. Частота обнаружения ботов относительно низка по сравнению с традиционными вредоносными программами. Например, ботнет Kraken был не замечен 80% коммерческими антивирусными средствами. Таким образом, миллионы узлов Интернета связанны с деятельностью ботнетов, а фактический процент может быть еще выше. В дополнение, мониторинг узла в реальном времени на основе поведения, как правило, сопровождается значительными накладными расходами системы, за счет чего, такие решения могут стать менее привлекательными для конечных пользователей.

Таким образом, акцент лучше делать на сетевые решения обнаружения. Существующие исследования проблемы обнаружений вторжений основанных на сети предложили немало методов и систем. В качестве примера можно привести системы обнаружения вторжений (СОВ) основанных на сигнатурах Snort и Bro [12]. Они полагаются на большую базу сигнатур для идентификации попыток вторжения в сетевом трафике. Основной недостаток сигнатурных СОВ, похож на недостаток антивирусных средств, это невозможность определять новые атаки. Это обусловлено тем, что новые атаки ранее ни когда не встречались и соответственно не имеют сигнатур. СОВ основанные на анализе аномалий могут преодолеть это ограничение путем описания нормального, легитимного, трафика. Соответственно любое отклонение от этого описания будет считаться аномалией. Примерами таких систем являются PAYL и Anagram [12]. Эти системы изучают полезную нагрузку входящих пакетов, проводят n-граммный анализ и выявляют эксплойт в полезной нагрузке. Основной недостаток решений на основе анализа аномалий – это большое количество ложных срабатываний.

Некоторые из указанных выше методов обнаружения вторжений и ВПО могут быть полезны в обнаружении некоторых аномалий ботнетов, но сами по себе не очень подходят для обнаружения ботнетов по следующим причинам:

- большинство СОВ фокусируются на изучении входящего трафика на наличие признаков попыток вторжения точка-точка. Как правило, они обнаруживают начальные входящие попытки вторжения, огромная частота с которой они производят подобные сигналы тревоги в сетях, хорошо описаны. Тем не менее, отличить успешное заражение локального хоста от повседневного множества сканирования и попыток вторжения является сложной задачей, как и любой аспект сетевой обороны.
- ботнеты очень гибки. Жизненный цикл инфицирования может состоять из нескольких различных этапов. Однако существующие подходы рассматривают только некоторые определенные признаки, такие как сканирование, поэтому они имеют меньше шансов обнаружить ботнеты. Они могут вызывать ложные срабатывания, если узел, не являющийся ботом, производит активность схожую со сканированием.

Выявление ботнетов с использованием систем приманок.

Большая часть исследований ботнетов сосредотачивалась на понимании природы и всего потенциала угрозы ботнетов, например, на проблеме исследования размеров ботнета, проблеме сбора экземпляров ботов или отслеживания.

Исследования размеров ботнетов могут помочь понять их угрозу в целом, их потенциал и динамику развития. Кук и др. [13] провели несколько основных исследований динамики развития ботнетов. Дагон и др. [14] предложили использовать технику перехвата DNS для исследования ботнетов и отметили суточное поведение ботнетов. Барфорд и Ягнесваран [15] исследовали исходный код бота для формирования взгляда на ботнет изнутри. Они проанализировали структурные сходства, защитные механизмы, возможности управления крупных семейств ботов. В конечном итоге, результаты этих исследований помогают лучше понять природу ботнетов, но на процесс предотвращения их использования влияют только косвенно.

Для эффективного сбора информации о ботнете и его отслеживания исследователи часто используют методы приманки. К примеру, приманка низкого уровня взаимодействия Nepenthes [16], которая имитирует несколько уязвимостей и автоматизирует сбор бинарных файлов ВПО. Использование приманок позволяет обеспечить углубленное изучение текущей деятельности ботнетов. Используя метод приманки исследователи могут собирать экземпляры ботов. Дальнейший анализ бинарных файлов позволяет формировать сигнатуры для контентного ботнета, либо получать информацию о C&C серверах (например, DNS sinkhole).

Хотя приманки и являются эффективным инструментом для сбора информации о ботнетах,

они имеют ряд ограничений. Во-первых, приманки низкого взаимодействия, такие как Nepenthes, могут отлавливать атаки только ограниченного числа известных эксплойтов, для которых они специально имитируют уязвимую среду. Приманки высокого уровня взаимодействия могут также не реализовывать всех сервисов, также не решает проблему масштабирования. Во-вторых, приманки, как правило, предназначены для захвата вредоносных программ распространяющихся с помощью сканирования удаленных уязвимостей, поэтому они не захватывают ВПО использующее другие способы распространения, таких как электронная почта или атака типа «Web drive-by download», которые являются двумя из самых популярных методов распространения [17]. В третьих, нет никакой гарантии частоты или объема получения ВПО с помощью этого подхода, т.к. приманка может только ждать и надеяться, что ВПО сама свяжется с ней. В четвертых, ВПО может избежать сканирования сети с «хорошо известными» приманками, определить окружение виртуальных машин, часто используемых для разворачивания приманок и изменить свое поведение, чтобы избежать анализа. Наконец, приманки сообщают об инфекциях только на машинах-ловушках, они не могут сообщить о заражении машины не являющейся ловушкой и функционирующей в корпоративной сети. Эти недостатки ограничивают использование приманок в качестве эффективных систем обнаружения.

Таким образом, по-прежнему существует необходимость в новых методах, которые больше подходят для обнаружения ботнетов. Традиционные техники обнаружения вторжений и ВПО полезны для обнаружения определенных признаков ботнетов. Некоторые из этих существующих методов могут быть компонентом новой системы, которая будет сочетать их с новыми методами обнаружения. Как показано в первом разделе статьи, ботнет – это сложная многоагентная система с элементами интеллектуальной работы. На этапе их распространения проводится автоматическая процедура анализа программного обеспечения пользователя на предмет имеющихся уязвимостей, эксплуатацию которых можно использовать для заражения. После заражения также решаются сложные задачи: определение используемых пользователем защитных систем, их обход, скрытие своей работы, взаимодействие с управляющими серверами. Для защиты от ботнетов необходимо использовать систему защиты с уровнем сложности не меньше, чем у самих ботнетов. Это значит необходимо применять метод и систему способную работать таким же распределенным способом, как и ботнет. Система должна обеспечивать возможность анализировать множество сетевых данных в разных сетях, обнаруживать сетевые атаки, влиять на фильтрацию трафика, выявлять сигнатуры вредоносного поведения и взаимодействовать между собой для эффективного выполнения перечисленных задач.

Многоагентная система защиты от ботнетов

Идея многоагентной системы защиты достаточно проста. Необходимо иметь возможность обнаруживать производимую ботнетом атаку, блокировать её, анализировать трафик зараженных машин, выявлять управляющий трафик ботнета, автоматически формировать сигнатуру ботнета и уже по ней обнаруживать всех ботов. Структура такой многоагентной системы приведена на рисунке 2. Данная многоагентная система имеет множество агентов обнаружения атак, множество агентов блокирования атак, множество агентов координации, множество агентов кластеризации трафика и формирования сигнатур, множество агентов обнаружения ботов и агентов мониторинга.

Каждый из агентов имеет модуль кооперации. Этот модуль необходим агентам для реализации взаимодействия между друг другом. Посредством этого модуля агенты обмениваются данными между собой и передаю команды управления в случае поддержки таковых. Агент обнаружения атаки содержит модуль обнаружения атак, помогающий обнаружить атаку, сформировать список атакующих узлов и передать его для обработки другим агентам. Агент блокирования атаки, принимая список узлов замеченных в проведении атаки, формирует запрещающее правило фильтрации трафика атаки и применяет его в модуле блокирования атаки. Для автоматической генерации сигнатуры злонамеренного трафика используется разработанный авторами алгоритм Botnet MultiAgent Recognition (BNMAR). Задача решается средствами агентов двух типов: агентом кластеризации трафика атакующей машины и агентом формирования сигнатур. Агент кластеризации трафика атакующей машины, используя модуль кластеризации, агрегирует весь трафик за определенный период и кластеризует его, после чего передаёт получившиеся кластера агенту формирования сигнатур. Агент формирования сигнатур с помощью модуля кросс-кластерной корреляции про-

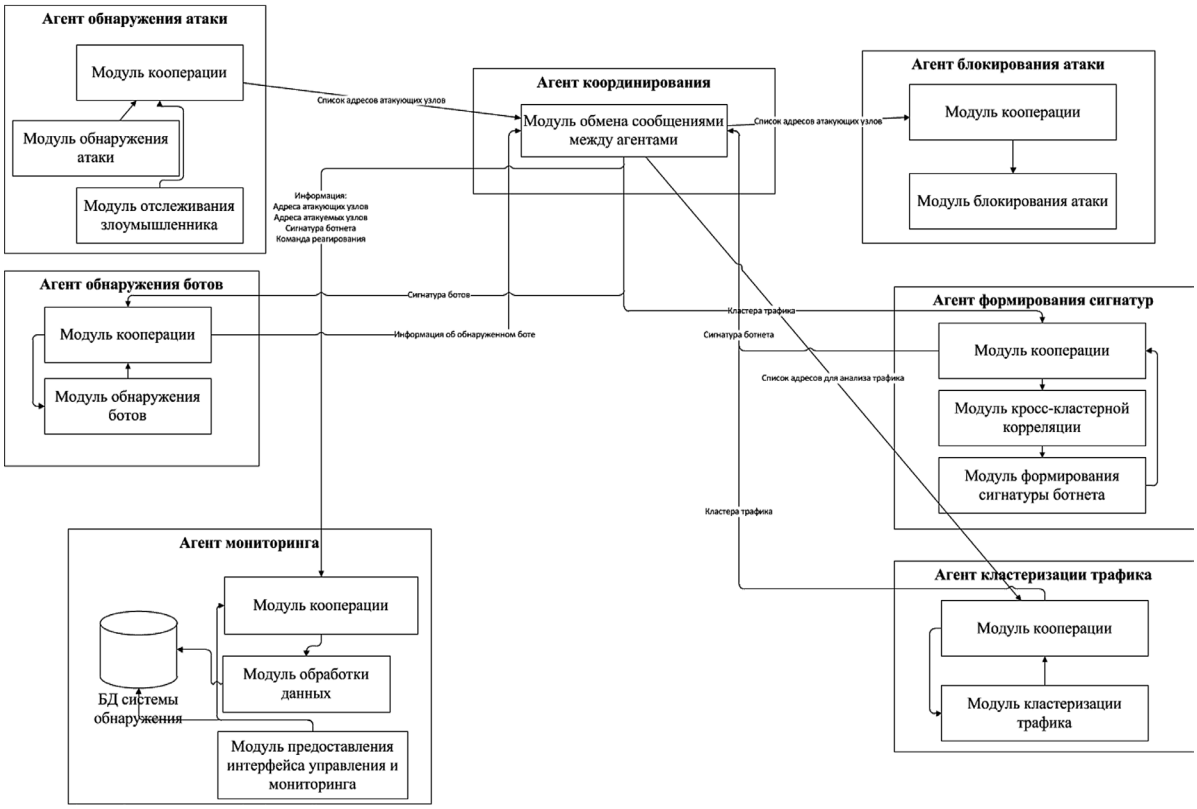

Рис.2. *Структура многоагентной системы защиты*

водит кросс-кластерную корреляцию кластеров полученных в результате анализа трафика всех узлов замеченных в одной атаке и генерирует сигнатуру для распознавания ботов посредством модуля формирования сигнатур.

Агент обнаружения ботов состоит из одноименного модуля. Агент мониторинга состоит из следующих модулей: модуль обработки данных, модуль предоставления интерфейса управления и мониторинга и базы данных. И последний агент координирования, отвечающий за обеспечение кооперации агентов, состоит из модуля обмена сообщениями.

Разработка исследовательского прототипа с нуля не имеет смысла, так как задачи многих агентов решаются различными зарекомендовавшими себя средствами с открытым исходным кодом. Соответствие модулей агентов и классом систем приведены в Таблице 1.

Таким образом, для большинства функций агентов можно использовать готовые системы с открытым исходным кодом. Разработки требуют модуль кооперации, модуль отслеживания злоумышленника, модуль кластеризации трафика, модуль кросс-кластерной корреляции и модуль формирования сигнатуры ботнета. Диаграмма развертывания прототипа данной системы приведена на рисунке 3.

Основные типы агентов (обнаружения и блокирования атак, кластеризации трафика, обна-

Таблица 1. *Соответствие модулей агентов классам систем*

Модуль агентов	Класс системы
Модуль обнаружения атаки	Система обнаружения атак
Модуль блокирования атаки	Межсетевой экран
Модуль обнаружения ботов	Система обнаружения ботов
Модуль обмена сообщениями	Связующее программное обеспечение
Модуль обработки данных	Диспетчер бинарных файлов событий СОВ
Модуль предоставления интерфейса управления и мониторинга	Система мониторинга безопасности сети

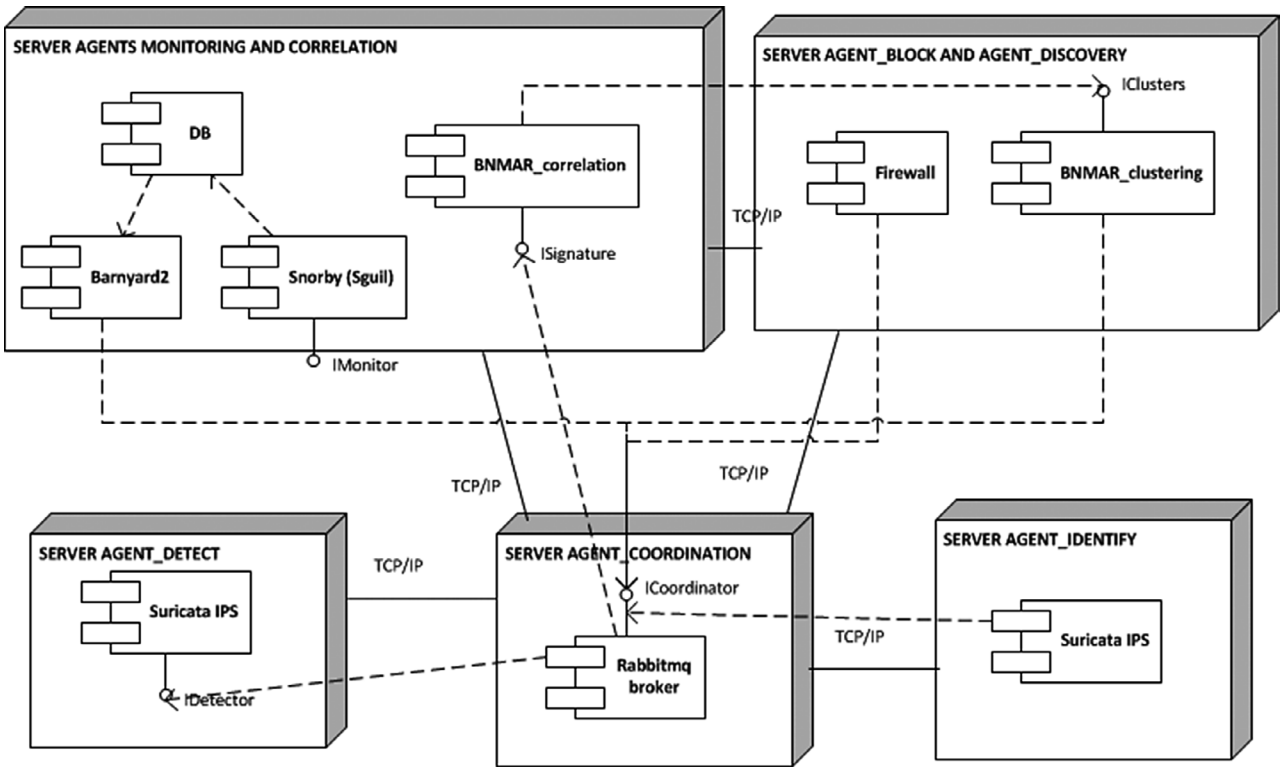

***Рис.3**. Диаграмма развертывания прототипа системы защиты*

ружения ботов, координации) могут эксплуатироваться в совершенно различных местах. Их можно было бы устанавливать множеству субъектам, начиная от обычных конечных пользователей и заканчивая любыми организациями, заинтересованными в своей защите, в том числе и в сетях провайдеров. Конечным пользователям можно предложить устанавливать агентов на своих компьютерах в виде модулей антивирусного программного обеспечения. Коммерческим организациям можно внедрять агентов на границе своих сетей, провайдеры могут расположить агентов в различных сетевых сегментах. Бизнесу было бы удобно использовать эту систему в виде дополнений к сетевому оборудованию различных производителей, таких как Cisco, CheckPoint, Mikrotik, Juniper и др.

Агенты мониторинга и формирования сигнатур могут располагаться в сети Интернет с обеспечением резервирования на серверах подконтрольных организации владеющей правами на управление и распространение многоагентной системы обнаружения ботов.

Заключение

В настоящей работе рассматривается проблема защиты информационных систем от ботнет атак. С использованием существующих методов не удается построить эффективную защиту. В работе предлагается использовать многоагентную систему обнаружения и блокирования ботнетов. Так как угрозу ботнета, как многоагентной системы, можно предотвратить использую такую же многоагентную систему. Обнаружение происходит на этапе взаимодействия и выполнения атаки жизненного цикла ботнета. Работа на этапе выполнения атаки может показаться малоэффективной в связи с уже случившимся фактом атаки, следовательно, ущерб, в каком-то объеме, узлам и сетям уже нанесен. С другой стороны, мы приобретаем возможность зафиксировать адреса скомпрометированных узлов, что дает нам преимущество в анализе трафика этих узлов и возможность выявить трафик этапа взаимодействия. Что, в конечном счете, позволяет формировать сигнатуру ботнета по управляющему трафику и обнаруживать ботов по всей глобальной сети.

***Рецензент**: Цирлов Валентин Леонидович, кандидат технических наук, доцент МГТУ им. Н.Э.Баумана, г. Москва, v.tsirlov@bmstu.ru*

Литература

1. M. Balduzzi, V. Ciangaglini, and R. McArdle, «Targeted attacks detection with SPuNge,» 2013 11th Annu. Conf. Privacy, Secur. Trust. PST 2013, pp. 185–194, 2013.
2. W. Lee, C. Wang, and D. Dagon, Botnet Detection: Countering the Largest Security Threat. Springer Publishing Company, Incorporated, 2010.
3. P. M. Gibbs, «Botnet Tracking Tools,» SANS Inst., 2014.
4. B. Marczak, N. Weaver, J. Dalek, R. Ensafi, D. Fiflield, S. McKune, A. Rey, J. Scott-Railton, R. Deibert, and V. Paxson, «China's Great Cannon,» no. April, pp. 1–19, 2015.
5. R. Rodrıguez-Gómez, «Analysis of Botnets Through Life-Cycle,» Ceres.Ugr.Es, pp. 257–262, 2011.
6. R. A. Rodríguez-Gómez, G. Maciá-Fernández, and P. García-Teodoro, «Survey and taxonomy of botnet research through life-cycle,» ACM Comput. Surv., vol. 45, no. 4, pp. 1–33, Aug. 2013.
7. C. Rossow, D. Andriesse, T. Werner, B. Stone-Gross, D. Plohmann, C. J. Dietrich, and H. Bos, «SoK: P2PWNED - Modeling and Evaluating the Resilience of Peer-to-Peer Botnets,» in 2013 IEEE Symposium on Security and Privacy, 2013, pp. 97–111.
8. Гайворонская С.А. Исследование методов обнаружения шеллкодов в высокоскоростных каналах передачи данных: автореферат дис. ... кандидата физико-математических наук: 05.13.11 / Московский государственный университет им. М.В. Ломоносова (МГУ). Факультет вычислительной математики и кибернетики. Москва, 2014.
9. M. Cova, C. Kruegel, and G. Vigna, «Detection and analysis of drive-by-download attacks and malicious JavaScript code,» in Proceedings of the 19th international conference on World wide web - WWW '10, 2010, p. 281.
10. Тарасов В.Б. От многоагентных систем к интеллектуальным организациям: философия, психология, информатика. М.: Эдиториал УРСС, 2002. 352 с.
11. Котов В.Д., Васильев В.И. Современное состояние проблемы обнаружения сетевых вторжений // Вестник Уфимского государственного авиационного технического университета. 2012. Т. 16. № 3 (48). С. 198-204.
12. P. Duessel, C. Gehl, P. Laskov, J.-U. Busser, C. Stoermann, and J. Kaestner, «Cyber-Critical Infrastructure Protection Using Real-Time Payload-Based Anomaly Detection,» Crit. Inf. Infrastructures Secur., vol. 6027, pp. 85–97, 2010.
13. E. Cooke, F. Jahanian, D. Mcpherson, and O. Ponomarev, «The Zombie Roundup: The Zombie Roundup: Understanding, Detecting, and Understanding, Detecting, and Disrupting Botnets Disrupting Botnets».
14. D. Dagon, C. C. Zou, and W. Lee, «Modeling Botnet Propagation Using Time Zones.,» Ndss, vol. 6, pp. 2–13, 2006.
15. P. Barford and V. Yegneswaran, «An Inside Look at Botnets,» in Malware Detection, Boston, MA: Springer US, 2007, pp. 171–191.
16. P. Baecher, M. Koetter, T. Holz, M. Dornseif, and F. Freiling, «The Nepenthes Platform: An Efficient Approach to Collect Malware,» Springer Berlin Heidelberg, 2006, pp. 165–184.
17. V. L. Le, I. Welch, X. Gao, and P. Komisarczuk, «Anatomy of drive-by download attack,» Proc. Elev. Australas. Inf. Secur. Conf. - Vol. 138, pp. 49–58, 2013.

ISSUES OF PROTECTING BUSINESS INFORMATION SYSTEMS FROM BOTNETS ATTACKS

Kosenko M.Yu.[3], Melnikov A.V.[4]

Malicious software that autonomously and automatically running on infected computers that form botnets used as the basic platform for the execution distributed attacks on various information systems. Using botnets, malicious users are realised various criminal activities: distributed denial of service, spaming, phishing, click fraud, theft of information, dissemination of other unwanted programs, abuse hosting. Traditional intrusion detection methods and malicious software are useful to detect certain characteristics of botnets, but as such, are not focused on the implementation of effective measures to prevent them. This article discusses six steps Botnet life–cycle and shows that from the point of view of artificial intelligence botnet can be regarded as multi–agent system. Various methods of protection against botnets were analyzed, advantages and disadvantages of these methods were presented. A multi–agent system detection and blocking botnets were proposed, the structure of the system were showed and the scheme of deployment of the system prototype was presented. The approaches of detection botnet on stages of interaction and implementation of the attack were presented in the context of the life cycle of the botnet.

Keywords: botnet detection, defense against botnets, botnet life–cycle, multi–agent protection system, intrusion detection system

3 Maxim Kosenko, Chelyabinsk State University, Chelyabinsk, kosenko@csu.ru

4 Andrey Melnikov, Dr.Sc., professor, Chelyabinsk State University, Chelyabinsk, mav@csu.ru

Reference

1. M. Balduzzi, V. Ciangaglini, and R. McArdle, «Targeted attacks detection with SPuNge,» 2013 11th Annu. Conf. Privacy, Secur. Trust. PST 2013, pp. 185–194, 2013.
2. W. Lee, C. Wang, and D. Dagon, Botnet Detection: Countering the Largest Security Threat. Springer Publishing Company, Incorporated, 2010.
3. P. M. Gibbs, «Botnet Tracking Tools,» SANS Inst., 2014.
4. B. Marczak, N. Weaver, J. Dalek, R. Ensafi, D. Fiflield, S. McKune, A. Rey, J. Scott-Railton, R. Deibert, and V. Paxson, «China's Great Cannon,» no. April, pp. 1–19, 2015.
5. R. Rodrıguez-Gómez, «Analysis of Botnets Through Life-Cycle,» Ceres.Ugr.Es, pp. 257–262, 2011.
6. R. A. Rodríguez-Gómez, G. Maciá-Fernández, and P. García-Teodoro, «Survey and taxonomy of botnet research through life-cycle,» ACM Comput. Surv., vol. 45, no. 4, pp. 1–33, Aug. 2013.
7. C. Rossow, D. Andriesse, T. Werner, B. Stone-Gross, D. Plohmann, C. J. Dietrich, and H. Bos, «SoK: P2PWNED - Modeling and Evaluating the Resilience of Peer-to-Peer Botnets,» in 2013 IEEE Symposium on Security and Privacy, 2013, pp. 97–111.
8. Gayvoronskaya S.A. Issledovanie metodov obnaruzheniya shellkodov v vysokoskorostnykh kanalakh peredachi dannykh: avtoreferat dis. ... kandidata fiziko-matematicheskikh nauk: 05.13.11 / Moskovskiy gosudarstvennyy universitet im. M.V. Lomonosova (MGU). Fakul'tet vychislitel'noy matematiki i kibernetiki. Moskva, 2014.
9. M. Cova, C. Kruegel, and G. Vigna, «Detection and analysis of drive-by-download attacks and malicious JavaScript code,» in Proceedings of the 19th international conference on World wide web - WWW '10, 2010, p. 281.
10. Tarasov V.B. Ot mnogoagentnykh sistem k intellektual'nym organizatsiyam: filosofiya, psikhologiya, informatika. Moscow: Editorial URSS, 2002. 352 P.
11. Kotov V.D., Vasil'yev V.I. Sovremennoe sostoyanie problemy obnaruzheniya setevykh vtorzheniy, Vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta. 2012. T. 16. No 3 (48), pp. 198-204.
12. P. D'uessel, C. Gehl, P. Laskov, J.-U. Busser, C. Stoermann, and J. Kaestner, «Cyber-Critical Infrastructure Protection Using Real-Time Payload-Based Anomaly Detection, «Crit. Inf. Infrastructures Secur., vol. 6027, pp. 85–97, 2010.
13. E. Cooke, F. Jahanian, D. Mcpherson, and O. Ponomarev, «The Zombie Roundup: The Zombie Roundup: Understanding, Detecting, and Understanding, Detecting, and Disrupting Botnets Disrupting Botnets».
14. D. Dagon, C. C. Zou, and W. Lee, «Modeling Botnet Propagation Using Time Zones.,» Ndss, vol. 6, pp. 2–13, 2006.
15. P. Barford and V. Yegneswaran, «An Inside Look at Botnets,» in Malware Detection, Boston, MA: Springer US, 2007, pp. 171–191.
16. P. Baecher, M. Koetter, T. Holz, M. Dornseif, and F. Freiling, «The Nepenthes Platform: An Efficient Approach to Collect Malware,» Springer Berlin Heidelberg, 2006, pp. 165–184.
17. V. L. Le, I. Welch, X. Gao, and P. Komisarczuk, «Anatomy of drive-by download attack,» Proc. Elev. Australas. Inf. Secur. Conf. - Vol. 138, pp. 49–58, 2013.