УДК 004.056 + 004.7.056

ИССЛЕДОВАНИЕ МЕТОДОВ ЗАЩИТЫ ОТ КИБЕРАТАК СИСТЕМЫ БОТНЕТ

В.К. Исмагамбетова, А.Д. Плетенкова, В.Ю. Бердюгин

Компьютерные сети, состоящие из зараженных вредоносными программами – ботами компьютеров, используются для совершения атак на информационные системы. Ботнеты используются для различных целей: атака типа «отказ в обслуживании», рассылка спама, кража информации. Для обнаружения вторжений и защиты от системы ботнет проведен анализ ряда методов.

Ключевые слова: защита от ботнет, антивирусные инструменты, система обнаружения вторжений, система приманок, многоагентная система защиты.

Развитие информационных технологий и внедрение их в различные сферы деятельности человека приводят к появлению новых видов киберпреступлений.

В настоящее время одним из главных инструментов киберпреступников стали ботнеты. Ботнет – своеобразная «зомби-сеть», созданная вирусом через уязвимости в программном обеспечении из-за невнимательности, неопытности пользователя, что позволяет злоумышленнику удаленно управлять зараженным компьютером, без ведома его владельца.

В 2016 году внимание специалистов по кибербезопасности привлекла система ботнет Mirai. Ее особенность – взлом не компьютеров, а иных «умных» устройств, включая камеры, термостаты и прочее с последующим использованием этих девайсов в качестве ботов для осуществления DDoS-атак. Первая версия Mirai включала около 400–500 тысяч подключенных устройств.

Ботнет-атаки представляют угрозу как для простых граждан (например, списание средств с их банковских счетов), так и коммерческих организаций, и государственных органов. В ряде случаев такие атаки могут представлять угрозу государственной безопасности.

Список возможностей ботнетов сам по себе довольно большой, но в основном все они исходят из нижеприведенных:

- Downloader – присутствует в большинстве вирусов. Обновляет старые версии бота, загружает через сеть практически любой контент (новые боты, трояны). Кроме того, на все компьютеры одновременно могут устанавливаться троянские программы, которые крадут все пароли, когда-либо введенные на данном компьютере.
- Keylogger – считывание введенных на клавиатуре символов с последующей отправкой злоумышленнику.
- DDoS (Distributed Denial of Service «отказ в обслуживании») – атака ресурса сети Интернет или компьютера путем множественных запросов от ботов с целью отказа в принятии и обработки запросов легитимных пользователей.
- Spam – рассылка спам-сообщений на электронные адреса пользователей. Более 95 % электронной почты в сети Интернет является спамом. Большинство этих сообщений спама, на самом деле, отправлены из ботнетов [1].
- Proxy – позволяет использовать любой компьютер из ботнета как прокси-сервер с целью сокрытия реального адреса злоумышленника.

Существует незаконное коммерческое применение ботнет. Ряд компаний его покупает или берет в аренду для рассылки спама и т.п.

Киберпреступники используют ботнет в целях получения финансовых средств, для ведения недобросовестной конкуренции, коммерческого шпионажа. Целью может быть и внесение хаоса в деятельность органов государственной власти.

Выявление и пресечение преступлений с использованием ботнет осуществляют государственные органы, в составе которых есть специализированные подразделения (например, Управление компьютерной и информационной безопасности Федеральной службы безопасности Российской Федерации, Управление «Р» и Управление «К» Министерства внутренних дел Российской Федерации). Так, в ноябре 2015 года сотрудники Управления «К» МВД России и отдела «К» ГУ МВД России по Нижегородской области совместно с оперативниками ЦИБ ФСБ России пресекли деятельность группы лиц, похищавших средства со счетов клиентов одного из крупнейших российских банков. Преступники использовали вредоносную программу для смартфонов, работающих на операционной системе «Андроид», что позволило им в короткие сроки создать бот-сеть, состоящую из более чем 16 тысяч скомпрометированных мобильных устройств.

Вместе с тем, данные явления приобрели такие масштабы, что сформировалась необходимость обучения технических специалистов и рядовых пользователей методам противодействия ботнету.

Для обнаружения вторжений и защиты от системы ботнет специалистами в сфере информационной безопасности разрабатываются различные ме-

тоды. Проблемами борьбы с ботнетом занимаются специализированные организации, например, «Лаборатория Касперского», ФГУП НИИ «Квант». Для эффективного применения таких методов необходимо знать их «плюсы» и «минусы». Некоторые из них будут проанализированы в данной работе.

Действующие техники обнаружения вторжений и вредоносного программного обеспечения можно объединить в следующие группы:

- решения, функционирующие на узлах;
- сетевые решения [2].

Антивирусные инструменты являются распространенным методом распознавания вредоносного программного обеспечения, который функционирует на узлах. Они полезны для традиционного обнаружения вирусов в течение длительного времени.

Еще одним методом обнаружения вторжения на узлах является мониторинг системных вызовов.

Вместе с тем при применении данных методов время от времени возникают проблемы обнаружения ботнетов. Данные методы основаны исключительно на анализе узла и имеют следующие проблемы:

- антивирусные инструменты основаны на поиске сигнатур, что требует объемную, точную и часто обновляемую базу сигнатур.
- системы обнаружения на узлах находятся на том же уровне привилегий, что и боты на некотором узле.

Примером решения вопросов выявления вторжения в сетях является система обнаружения вторжений. Это, в свою очередь, большая группа отдельных методов (например, анализ аномалий, анализ изменения состояний и многие другие), позволяющих собирать и анализировать информацию из различных точек защищаемой сети для обнаружения вторжений [3]. Они основаны на большой базе сигнатур для определения попыток вторжения в сетевой трафик.

Системы обнаружения вторжений, основанные на анализе аномалий, могут преодолевать ограничение, когда новая атака не имеет сигнатур. Это достигается путем описания нормального трафика, и отклонение от описания будет считаться аномалией.

Большое количество ложных срабатываний является основной проблемой решений на основе анализа аномалий.

Вместе с тем, для эффективной борьбы с системой ботнет необходимо ее исследование. Одним из способов является сбор экземпляров ботов и их отслеживание методом приманки.

Приманки углубленно изучают текущую деятельность ботнетов. Этот метод является эффективным инструментом в сборе информации о ботнете, но он все же имеет свои минусы. В основном приманки используют для выявления атак только ограниченного количества известных эксплойтов, а также они используются для захвата вредоносных программ, которые распространяются с помощью сканирования удаленных уязвимостей [4].

Поэтому система приманок не может захватить вредоносные программы, пользующиеся другими методами распространения. Основной принцип работы приманок заключается в том, что они могут только ждать и надеяться, что вредоносное программное обеспечение само свяжется с ней.

Некоторые вредоносные программные обеспечения могут изменять свое поведение, чтобы избегать сканирования систем-приманок. Приманки не могут сообщать о заражении машины, которая функционирует в корпоративной сети и не является машиной-ловушкой. Эти ограничения снижают эффективность систем обнаружения.

Поэтому для защиты от ботнетов нужно использовать систему защиты с уровнем сложности не меньше, чем у самих ботнетов. Система должна уметь анализировать сетевые данные в разных сетях, обнаруживать сетевые атаки, выявлять вредоносное поведение и взаимодействовать между собой для эффективного выполнения перечисленных задач. Необходимость выявлять производимую ботнетом атаку, блокировать ее, анализировать зараженные машины, выявлять управляющий трафик ботнета, формировать сигнатуру ботнета и по ней обнаруживать ботов – главная идея многоагентной системы.

Многоагентная система имеет множество агентов обнаружения атак, множество агентов блокирования атак, множество агентов координирования, множество агентов кластеризации трафика и формирования сигнатур, множество агентов обнаружения ботов и агентов мониторинга. Каждый из них имеет модуль кооперации, который помогает взаимодействовать агентам между собой, передавая данные и команды управления.

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.

Агент кластеризации трафика атакующей машины, используя модуль кластеризации, агрегирует весь трафик за определенный период и кластеризует его, после чего передает получившиеся кластера агенту формирования сигнатур.

Агент формирования сигнатур с помощью модуля кросс-кластерной корреляции проводит кросс-кластерную корреляцию 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 модуля кооперации.

И последний агент координирования, отвечающий за обеспечение кооперации агентов, состоит из модуля обмена сообщениями [4].

В многоагентной системе обнаружение происходит на начальном этапе взаимодействия и выполнения атак ботнета. Обеспечение защиты на этапе выполнения атаки рискованно, так как ущерб в каком-то объеме узлам и сетям уже нанесен. С другой стороны, мы получаем возможность определить адреса скомпрометированных узлов и выявить трафик взаимодействия. Это в итоге позволяет обнаруживать ботов по всей сети и формировать сигнатуры ботнета по управляющему трафику.

Таким образом, в настоящее время разработаны различные методы обнаружения вторжений, которые могут использоваться для защиты от ботнет. Однако эти методы имеют различную эффективность.

Традиционные техники обнаружения вторжений и вредоносного программного обеспечения полезны для выявления определенных признаков ботнетов. Вместе с тем, для методов, основанных на анализе локальных узлов, характерны следующие недостатки:

- большое количество ложных срабатываний, пропусков атак и слабые возможности по обнаружению новых атак;
- невозможность определить вторжения на начальном этапе;
- трудность определения атакующего и цели атаки;
- сложность и затратность обнаружения атаки в реальном времени.

Системы приманок являются эффективными для сбора данных о ботнете, но работают с немногими типами распространения.

Наиболее эффективной в настоящее время является многоагентная система. Она не дает ложных срабатываний при аномалиях трафика сети, не требует частого обновления базы сигнатур (в отличие от систем, работающих на локальных узлах), работает с многими типами распространения (в отличие от систем приманок).

Библиографический список

1. Косенко, М.Ю. Вопросы обеспечения защиты информационных систем от ботнет атак / М.Ю. Косенко, А.В. Мельников // Вопросы кибербезопасности. – 2016. – № 4(17). – С. 20–28.

2. Котов, В.Д. Современное состояние проблемы обнаружения сетевых вторжений / В.Д. Котов, В.И. Васильев // Вестник Уфимского государственного авиационного технического университета. – 2012. – Т. 16. № 3 (48). – С. 198–204.

3. Корниенко, А.А. Системы обнаружения вторжений: современное состояние и направления совершенствования / А.А. Корниенко, И.М. Слюсаренко // Проблемы информационной безопасности. Компьютерные системы. – 2004. – № 1. – С. 21–34.

4. Косенко, М.Ю. Многоагентная система обнаружения и блокирования ботнетов путем выявления управляющего трафика на основе интеллектуального анализа данных: дис… канд. тех. наук / М.Ю. Косенко. – Челябинск, 2017. – 149 с.

К содержанию