РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 703 329**(13) **C1**

(51) МПК
H04L 29/06 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 29/06 *(2019.08);* ***H04L 63/1408*** *(2019.08);* ***H04L 63/1416*** *(2019.08);* ***H04L 63/1425*** *(2019.08);* ***H04L 63/1458*** *(2019.08)*

(21)(22) Заявка: **2018142311, 30.11.2018**

(24) Дата начала отсчета срока действия патента:
30.11.2018

Дата регистрации:
16.10.2019

Приоритет(ы):
(22) Дата подачи заявки: **30.11.2018**

(45) Опубликовано: **16.10.2019** Бюл. № **29**

Адрес для переписки:
127287, Москва, Старый Петровско-Разумовский пр-д, 1/23, стр. 1, Открытое акционерное общество "Информационные технологии и коммуникационные системы"

(72) Автор(ы):
Гурина Анастасия Олеговна (RU),
Елисеев Владимир Леонидович (RU)

(73) Патентообладатель(и):
Открытое акционерное общество "Информационные технологии и коммуникационные системы" (RU)

(56) Список документов, цитированных в отчете о поиске: **US 9661019 B2, 23.05.2017. CN 107800727 A, 13.03.2018. US 9167004 B2, 20.10.2015. US 2005/0249214 A1, 10.11.2005. RU 2649290 C1, 30.03.2018.**

(54) Способ обнаружения несанкционированного использования сетевых устройств ограниченной функциональности из локальной сети и предотвращения исходящих от них распределенных сетевых атак

(57) Реферат:

Изобретение относится к области вычислительной техники. Техническим результатом является обнаружение несанкционированного использования сетевых устройств ограниченной функциональности из локальной сети и предотвращение исходящих от них распределенных сетевых атак на сетевые узлы в глобальной сети непосредственно в источнике атаки. Способ обнаружения несанкционированного использования сетевых устройств ограниченной функциональности и предотвращения распределенных атак заключается в том, что устройства ограниченной функциональности отправляют в модуль анализа шлюза защищенное от подмены сообщение, содержащее собственный сетевой адрес, при обнаружении собственной аномальной активности; в модуле анализа проверяют, являются ли сообщения аутентичными; вычисляют параметр, характеризующий взаимосвязь между аутентичными сообщениями; проверяют в модуле анализа выполнение условия несанкционированного использования устройств ограниченной функциональности, и если условие выполнено, то формируют список сетевых адресов устройств ограниченной функциональности, для которых сделан вывод об их несанкционированном использовании, запрашивают у шлюза сетевой трафик перечисленных в списке устройств, анализируют сетевую активность перечисленных в списке устройств на предмет признаков исходящей распределенной атаки, в случае обнаружения которой формируют правила фильтрации сетевого трафика, применяют правила фильтрации в шлюзе, предотвращая скоординированную распределенную сетевую атаку со стороны сетевых устройств ограниченной функциональности до тех пор, пока в модуле анализа шлюза выполняется условие

RU 2703329 C1

RU 2703329 C1

несанкционированного использования устройств. 9 з.п. ф-лы.

RU 2703329 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 703 329**(13) **C1**

(51) Int. Cl.
H04L 29/06 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 29/06 *(2019.08);* ***H04L 63/1408*** *(2019.08);* ***H04L 63/1416*** *(2019.08);* ***H04L 63/1425*** *(2019.08);* ***H04L 63/1458*** *(2019.08)*

(21)(22) Application: **2018142311, 30.11.2018**

(24) Effective date for property rights:
30.11.2018

Registration date:
16.10.2019

Priority:
(22) Date of filing: **30.11.2018**

(45) Date of publication: **16.10.2019** Bull. № **29**

Mail address:
127287, Moskva, Staryj Petrovsko-Razumovskij pr-d, 1/23, str. 1, Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy"

(72) Inventor(s):
Gurina Anastasiya Olegovna (RU),
Eliseev Vladimir Leonidovich (RU)

(73) Proprietor(s):
Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy" (RU)

RU 2703329 C1

(54) METHOD OF DETECTING UNAUTHORIZED USE OF NETWORK DEVICES OF LIMITED FUNCTIONALITY FROM A LOCAL NETWORK AND PREVENTING DISTRIBUTED NETWORK ATTACKS FROM THEM

(57) Abstract:

FIELD: computer engineering.

SUBSTANCE: invention relates to computer engineering. Method of detecting unauthorized use of network devices of limited functionality and prevention of distributed attacks consists in the fact that reduced functionality devices send a message-protected message containing a network address to the gateway analysis module when detecting intrinsic abnormal activity; in analysis module checking whether messages are authentic; calculating a parameter characterizing the relationship between authentic messages; checking in the analysis module the performance of the condition of unauthorized use of devices of limited functionality, and if the condition is met, then forming a list of network addresses of devices of limited functionality, for which there is a conclusion on their unauthorized use, requesting gateway network traffic listed in the list of devices, analyzing network activity listed in the list of devices for signs of outgoing distributed attack, in case of detection, rules of filtering network traffic are formed, filtering rules are applied in gateway, preventing coordinated distributed network attack on the side of network devices of limited functionality until conditions of unauthorized use of devices are fulfilled in gateway analysis module.

EFFECT: detection of unauthorized use of network devices of limited functionality from a local network and prevention of distributed network attacks on network nodes in a global network directly in the attack source.

10 cl

RU 2703329 C1

Область техники, к которой относится изобретение

Предлагаемое изобретение относится к области сетевой безопасности, в частности, к способам обнаружения несанкционированного использования сетевых устройств ограниченной функциональности для организации распределенных сетевых атак, основанным на обнаружении аномалий в работе сетевых устройств ограниченной функциональности, а также к способам предотвращения распределенных сетевых атак на сетевые узлы в глобальной сети со стороны сетевых устройств ограниченной функциональности.

Уровень техники

Состояние сетевой безопасности с учетом стремительного роста объемов выпуска и эксплуатации простых сетевых устройств, подключенных к Интернет, а также участившихся сетевых атак с их участием, вызывает все большее беспокойство в банковской, промышленной, государственной сфере и становится проблемой мирового масштаба.

Причиной сложившейся ситуации, в частности, является популяризация и повсеместное распространение Интернета Вещей (Internet of things, IoT) - концепции, которая связывает с Интернетом множество автономных приборов или физических объектов, способных собирать данные и обмениваться данными, поступающими со встроенных сервисов. Устройства, входящие в Интернет Вещей, или IoT устройства - это любые подключенные к Интернету автономные устройства, которые могут отслеживаться и/или управляться удаленно. Чаще IoT предназначен для использования конечным пользователем и применяется в таких продуктах, как “умная” бытовая техника, носимая электроника (фитнес-трекеры, “умные” часы) и пр.

Однако, Интернет Вещей включает в себя и Промышленный Интернет Вещей (Industrial Internet of things, IIoT) - концепцию, позволяющую оптимизировать работу компаний промышленного сектора посредством сети, состоящей из физических устройств (датчиков, сенсоров, контроллеров и т.д.) для выполнения конкретных задач на производстве, например, для интеллектуального обслуживания оборудования, сбора данных с датчиков и их анализа в реальном времени. IIoT проекты реализуются в различных отраслях экономики и имеют корпоративного потребителя, либо в роли потребителя выступает все общество в целом.

На основе устройств класса IoT создаются «умные» дома и города, интеллектуальные промышленные системы и сети, призванные повысить уровень жизни и производства за счет автоматизации процессов и сокращения материальных и временных затрат, необходимых для их выполнения стандартным способом. Однако устройства Интернета Вещей в силу своей компактности, многочисленности и узкой функциональной специализации, как правило, не рассматриваются как компьютерное оборудование, поэтому и средства защиты, подходящие для серверов, персональных компьютеров и даже мобильных телефонов, в них не устанавливаются. Производители устройств IoT не предусматривают возможностей для администрирования, обновления встроенного программного обеспечения (ПО) и включения таких средств защиты, как антивирусы, системы обнаружения вторжений (IDS) и предотвращения вторжений (IPS), поскольку вычислительные ресурсы таких устройств существенно ограничены и рассчитаны только на обеспечение функционирования устройства по назначению.

Массовое производство дешевых устройств этого класса обусловлено принципиально быстрой и малозатратной разработкой устройств с минимальным и простым функционалом, не предусматривающей включение каких-либо серьезных функций безопасности. Кроме того, установка таких устройств в большинстве случаев происходит

без привлечения специалистов по компьютерной безопасности. Часто встречаются случаи, когда целые серии устройств уже официально сняты с поддержки, но до сих пор широко эксплуатируются в быту и производстве. Все эти факторы в совокупности с такими неотъемлемыми свойствами IoT-устройств, как подключение к сети Интернет и осуществление коммуникаций через Интернет, добавляет серьезные проблемы с безопасностью, делая устройства уязвимыми к многочисленным сетевым угрозам, вторжениям и атакам. Таким образом, оказывается, что владелец устройства IoT даже при наличии квалификации в области информационной безопасности не имеет возможности контролировать работу устройства и усилить защиту устройства путем установки дополнительных программ, например, антивируса. Поэтому обнаружение проникновения и последующего злонамеренного использования устройства всегда проходят незамеченными.

В настоящее время практически незащищенные устройства с известными уязвимостями производятся довольно многочисленными сериями годами, что позволяет злоумышленникам, эксплуатируя уязвимости или пользуясь слабостью встроенных систем защиты, заражать устройства вредоносным ПО, обеспечивающим удаленное управление ими, создавать масштабные сети зараженных устройств - ботнеты, и использовать их как инструмент для проведения вредоносной активности и различных атак. Чаще всего ботнеты используют для организации распределенных атак типа «отказ в обслуживании» (Distributed Denial of Service, DDoS). В таком случае при получении команды из командного центра, IoT-устройства согласно программе ботнета начинают осуществлять атаку в отношении заданной цели, вызывая отказ в обслуживании, снижение производительности или переполнение пропускной способности канала. Обычно для переполнения канала используется любой вид пакетов TCP, ICMP или UDP, где адреса источников атаки - зараженных устройств, настоящие, и таким образом, практически неотличимые от подключающихся компьютеров реальных пользователей. Распределенные атаки, как известно, способны не только вывести из строя какой-то определенный сайт, сервис или систему, но и нарушить работу некоторого сегмента сети или, например, отключить Интернет в маленькой стране. В настоящее время DDoS-атаки случаются все чаще и их мощность с каждым разом существенно возрастает.

Существует множество рекомендаций для пользователей и производителей, которые могли бы повысить уровень защиты IoT-устройств, однако этого не происходит. В связи с этим возникает необходимость в принятии более серьезных мер.

Ряд исследователей и специалистов области информационной безопасности разрабатывают способы обнаружения и предотвращения распределенных сетевых атак типа DDoS, наиболее распространены способы, использующие различные варианты сигнатурного подхода.

Например, известен способ обнаружения и предотвращения DDoS атак [1], в котором на каждом узле защищаемой распределенной вычислительной сети установлен агент, выполненный с возможностью обращения к базе знаний, содержащей сведения об известных шаблонах атак. Агент контролирует события, связанные с ресурсами, и определяет путем кластерного анализа, являются ли эти события шаблонами известных или неизвестных атак, а также классифицирует атаки и инициирует ответные действия, включая отправку предупреждений и изменение пула ресурсов, при этом в случае обнаружения неизвестного шаблона атаки ответные действия выбираются случайным образом. Помимо недостатков, характерных для всех сигнатурных методов обнаружения атак, а именно: уязвимость перед модифицированными и новыми способами проведения

атак и значительные человеческие и аппаратные ресурсы, требующиеся для создания, хранения и постоянного обновления базы знаний известных шаблонов атак, способ имеет еще один серьезный недостаток, заключающийся в обнаружении атаки с задержкой - только после обнаружения ее известных признаков и последствий атакованными узлами сети.

Известен способ обнаружения DDoS-атак [2] на основе обнаружения аномалий, направленный на снижение задержки обнаружения, в котором используется технология Spark Streaming, сконфигурированная для поддержки измерения одновременно нескольких факторов, каждый из которых имеет свой собственный порог для обнаружения DDoS-атаки, при этом пороговое значение каждого из факторов настраивается с помощью машинного обучения. Способ хоть и позволяет избежать основных недостатков сигнатурных методов и снизить задержку обнаружения атак, но не обеспечивает их предотвращение в принципе.

Известны также способы [3, 4], в которых для обнаружения распределенных атак используется распределенный подход в обнаружении сетевых аномалий. При этом в решении, описанном в [3], обнаружение распределенной атаки обеспечивается за счет централизованного определения корреляции событий, но не обеспечивается предотвращение распределенной атаки, а в способе обнаружения и смягчения высокоскоростных распределенных атак типа «отказ в обслуживании», описанном в [4], для обнаружения атак используется пороговая логика, а после обнаружения осуществляется лишь смягчение последствий атаки.

Известные способы обеспечивают обнаружение распределенных атак только после выявления на стороне атакованных узлов защищаемой сети аномалий, вызванных последствиями осуществляемой атаки. Основными недостатками указанных способов является наличие задержки обнаружения распределенных атак и отсутствие возможности их полного предотвращения.

Учитывая тенденцию роста мощности IoT-ботнетов, являющихся источником лавинообразных вредоносных запросов, которые атакуемый сетевой ресурс не успевает обработать и вследствие которых происходит «отказ в обслуживании», критичным становится время задержки обнаружения и своевременное предотвращение таких распределенных атак. Критичность этого времени обусловлена значительными материальными убытками и репутационными рисками, к которым приводят секунды перебоев и простоев в работе систем, связанных с Интернетом, в особенности это актуально для стратегически важных организаций, в которых недопустим даже частичный и кратковременный выход из строя. Тот факт, что сайты органов власти, сайты ведущих IT-корпораций, сайты банков и другие сетевые ресурсы до сих пор продолжают подвергаться крупным распределенным атакам ботнетов, в частности, типа DDoS, и терпят существенные убытки, свидетельствует о том, что известные средства противодействия такого рода атакам недостаточно эффективны, и проблема до сих пор не решена.

Кроме того, необходимо отметить, что обнаружение и предотвращение распределенных атак в реальном масштабе времени на стороне атакуемого, особенно на высоких сетевых скоростях, требует значительного объема ресурсов, которые предоставляют только дорогостоящие и достаточно сложные технические решения, не являющиеся универсальными для применения в любой области.

Задача обнаружения и предотвращения распределенных атак может быть решена эффективнее, быстрее и без выделения значительных ресурсов на идентификацию и фильтрацию атакующего трафика, если обеспечить обнаружение исходящей

распределенной атаки в ее источнике и фильтровать атакующий трафик непосредственно в точке подключения источника атаки к Интернету, не допуская, тем самым, выход атакующего трафика в Интернет.

Раскрытие изобретения

Цель изобретения состоит в создании единого способа обнаружения несанкционированного использования устройств ограниченной функциональности, организованного для создания сети захваченных устройств и осуществления распределенных атак с их помощью, и раннего предотвращения распределенных сетевых атак непосредственно в их источнике.

Техническим результатом является обнаружение несанкционированного использования сетевых устройств ограниченной функциональности из локальной сети и предотвращение исходящих от них распределенных сетевых атак на сетевые узлы в глобальной сети непосредственно в источнике атаки.

Для этого предлагается способ обнаружения несанкционированного использования сетевых устройств ограниченной функциональности из локальной сети и предотвращения исходящих от них распределенных сетевых атак на сетевые узлы в глобальной сети, ранее описанный в [5], при этом локальная сеть, включает:

- шлюз, установленный на границе локальной сети, содержащий модуль анализа и выполненный с возможностью:
  - передачи трафика в ответ на запрос модуля анализа,
  - фильтрации трафика согласно принимаемым от модуля анализа правилам фильтрации;
- сетевые устройства ограниченной функциональности, имеющие в своем составе операционную систему и выполненные с возможностью:
  - выхода в глобальную сеть через шлюз,
  - обнаружения собственной аномальной активности,
  - формирования и передачи модулю анализа шлюза защищенного от подмены сообщения, раскрывающего сетевой адрес устройства ограниченной функциональности, при обнаружении им собственной аномальной активности;

причем модуль анализа выполнен с возможностью:

- предустановки признаков исходящей распределенной сетевой атаки,
- приема и обработки защищенных от подмены сообщений от сетевых устройств ограниченной функциональности,
- запроса, приема и анализа сетевого трафика устройств ограниченной функциональности,
- формирования правил фильтрации на основе анализа и их отправки на шлюз;

способ заключается в том, что

- задают в модуле анализа количество сетевых устройств ограниченной функциональности в локальной сети и допустимый уровень аномальной активности в локальной сети;
- определяют в модуле анализа условие несанкционированного использования сетевых устройств ограниченной функциональности;
- запускают сетевые устройства ограниченной функциональности и шлюз в рабочем режиме;
- получают в модуле анализа в режиме реального времени защищенные от подмены сообщения, содержащие сетевые адреса устройств ограниченной функциональности, обнаруживших свою аномальную активность;
- проверяют в модуле анализа полученные сообщения на аутентичность и

отбрасывают неаутентичные;

• вычисляют в режиме реального времени параметр, характеризующий взаимосвязь между полученными модулем анализа аутентичными сообщениями;

• проверяют в модуле анализа выполнение условия несанкционированного использования сетевых устройств ограниченной функциональности,

• если условие выполнено, то

◦ выполняют в модуле анализа следующие действия:

· формируют список сетевых адресов устройств ограниченной функциональности, для которых выполнено условие несанкционированного использования,

■ запрашивают у шлюза сетевой трафик устройств ограниченной функциональности, сетевые адреса которых перечислены в списке,

■ получают от шлюза сетевой трафик устройств ограниченной функциональности, сетевые адреса которых перечислены в списке,

■ анализируют сетевую активность посредством поиска в сетевом трафике устройств ограниченной функциональности, сетевые адреса которых перечислены в списке, признаков исходящей распределенной сетевой атаки,

■ формируют правила фильтрации сетевого трафика на основе анализа сетевой активности устройств ограниченной функциональности, сетевые адреса которых перечислены в списке,

■ передают правила фильтрации на шлюз;

◦ фильтруют сетевой трафик согласно полученным от модуля анализа правилам фильтрации с помощью шлюза, предотвращая скоординированную распределенную сетевую атаку со стороны сетевых устройств ограниченной функциональности, сетевые адреса которых перечислены в списке, до тех пор, пока в модуле анализа шлюза выполняется условие несанкционированного использования сетевых устройств ограниченной функциональности.

Под сетевыми устройствами ограниченной функциональности понимаются устройства класса IoT или любые другие сетевые устройства, обладающие следующими характеристиками:

1) устройство работает на базе компактных аппаратных средств с малым энергопотреблением, таких как микрокомпьютеры, микроконтроллеры;

2) устройство имеет операционную систему (ОС) с невысоким потреблением системных ресурсов (легковесную ОС) и ограниченный набор прикладных программ, не меняющийся на протяжении всего времени эксплуатации устройства по назначению;

3) устройство имеет постоянное подключение к стандартной коммуникационной среде, через которую с помощью Интернет-провайдера обеспечивается возможность глобальных сетевых коммуникаций;

4) сетевое взаимодействие устройства, необходимое для реализации функционального назначения устройства, ограничено минимальным набором сценариев, протоколов сетевого обмена, форматов входных и выходных данных, полностью определяемых на этапе производства и не меняющихся на протяжении всего времени эксплуатации устройства по назначению;

5) устройства одной модели идентичны и отличаются только серийным номером.

Подобные сетевые устройства ограниченной функциональности в зависимости от своего назначения выполняют заданный при производстве ограниченный набор функций зачастую даже в определенной и повторяющейся последовательности. Например, «умный» прибор учета ресурсов или подключенный к Интернету счетчик позволяет в режиме реального времени снимать показания расхода воды, электричества или газа

и передавать данные на сетевой или «облачный» сервер. Таким образом, для данного сетевого устройства ограниченной функциональности такая активность, включая определенные сценарии удаленного управления им с определенного доверенного сетевого адреса, является нормальной, а любая другая незапланированная разработчиком активность, например, отправка ранее не формируемых пакетов на ранее не используемый адрес, для него будет нетипична и аномальна.

Также аномальная активность сетевых устройств ограниченной функциональности может быть спровоцирована:

- аппаратными неисправностями;
- программными ошибками и сбоями;
- исчерпанием вычислительных ресурсов;
- аномалиями в сетевом взаимодействии.

Сетевая активность устройства ограниченной функциональности может стать аномальной в результате несанкционированного использования устройства, а именно:

- сканирования открытых портов;
- подбора паролей;
- фаззинга;
- эксплуатации уязвимостей устройства;
- инъекции кода;
- загрузки неизвестных, вредоносных файлов, ПО на устройство;
- попытки получения доступа к устройству и захвата управления устройством;
- принудительной генерации устройством нетипичного для его назначения трафика, атакующего трафика.

Интерактивный мониторинг аномальных событий - случаев обнаружения аномальной активности каждого сетевого устройства ограниченной функциональности из локальной сети в режиме реального времени, позволит выявлять случаи единовременных подозрительных событий в локальной сети, что, как известно, характерно для создания и использования ботнета из сетевых устройств ограниченной функциональности в целях организации с их помощью распределенной сетевой атаки на узел в глобальной сети.

Основная идея предлагаемого способа заключается в том, что подобная аномальная активность может быть обнаружена самим сетевым устройством ограниченной функциональности в режиме реального времени с помощью встроенного в его ПО классифицирующего модуля, способного выделять аномалии в признаках сетевого трафика, выходящие за пределы области признаков разрешенного сетевого взаимодействия устройства, заранее заложенной в классификаторе. Помимо модуля, детектирующего аномальную активность устройства, необходим коммуникационный модуль, который после получения сигнала от классификатора об обнаружении аномалии в режиме реального времени способен безопасным образом доставить специальные защищенные от подмены сообщения, предупреждающие об источнике аномальной активности. В таком случае, если защищенные от подмены сообщения от всех сетевых устройств ограниченной функциональности, находящихся в одной локальной сети и обнаруживших собственную аномальную активность, принимать на одном сетевом узле, установленном на границе локальной сети и обеспечивающем возможность глобальных сетевых коммуникаций, то можно выявлять случаи одновременного использования не по назначению, то есть несанкционированного использования, целого множества сетевых устройств ограниченной функциональности из локальной сети. Анализ трафика именно этих сетевых устройств ограниченной функциональности и обнаружение в нем известных признаков распределенной атаки позволяет сформировать

правила фильтрации, запрещающие атакующему трафику выход в глобальную сеть. Применение таких правил на сетевом узле позволит заблокировать атакующий трафик и предотвратить распределенные атаки, исходящие от захваченных сетевых устройств ограниченной функциональности и направленные на сетевые узлы глобальной сети, в точке, максимально близкой к ее источнику.

Необходимо отметить, что способ обеспечивает обнаружение несанкционированного использования только тех сетевых устройств ограниченной функциональности, которые находятся в пределах контролируемой модулем анализа шлюза сети - локальной сети. При этом локальная сеть может из себя представлять, как сеть, покрывающую относительно небольшую территорию, так и сеть, состоящую из сетевых устройств ограниченной функциональности, получающих доступ в глобальную сеть через одного Интернет-провайдера. Причем, когда локальная сеть - это сеть из клиентов поставщика Интернет-услуг, глобальная сеть представляет собой сеть Интернет, тогда шлюз, обеспечивающий сетевым устройствам ограниченной функциональности локальной сети выход в глобальную сеть Интернет, должен быть установлен на стороне поставщика Интернет-услуг.

В общем случае под глобальной сетью может быть принята либо сеть Интернет, либо сеть, имеющая в своем составе одну или более локальных сетей в качестве компонентов, то есть стоящая на уровень выше локальной сети в сетевой иерархии.

Для использования способа необходимы сетевые устройства ограниченной функциональности, имеющие в своем составе ОС и выполненные с возможностью:

- выхода в глобальную сеть через шлюз,
- обнаружения собственной аномальной активности,
- формирования и передачи модулю анализа шлюза защищенного от подмены сообщения, раскрывающего сетевой адрес устройства ограниченной функциональности при обнаружении им собственной аномальной активности.

Способность сетевых устройств ограниченной функциональности выявлять собственную аномальную активность и формировать защищенные от подмены сообщения, которые отправляются на модуль анализа шлюза при обнаружении собственной аномальной активности, обеспечивается за счет встроенного модуля обнаружения аномальной активности.

Рассмотрим выполнение модуля обнаружения аномальной активности, обеспечивающего сетевые устройства ограниченной функциональности необходимыми для осуществления способа возможностями.

Модуль обнаружения аномалий включает в себя два модуля: классифицирующий и коммуникационный, которые могут быть созданы и внедрены в ПО сетевого устройства ограниченной функциональности, как на стадии производства, так и непосредственно перед использованием способа.

Возможности сетевого устройства ограниченной функциональности в части обнаружения собственной аномальной активности реализуются за счет классифицирующего модуля. Классифицирующий модуль может быть сформирован следующим образом.

Так как прикладное назначение сетевых устройств ограниченной функциональности (далее устройств) зачастую однонаправленно и их функционал ограничен не большим набором типовых операций с применением одних и тех же специальных протоколов сетевого обмена, а входные и выходные данные имеют однотипный формат, то все сетевые взаимодействия такого устройства могут быть представлены в виде некоторой ограниченной области разрешенного сетевого взаимодействия, описываемой

совокупностью признаков входящего и исходящего сетевого трафика устройства при его использовании строго по назначению.

Принимая во внимание не меняющийся в процессе эксплуатации ограниченный функционал устройства, представляется возможным один раз за время эксплуатации устройства построить классификатор, распознающий на основе анализа признаков сетевого трафика, является ли активность нормальной, то есть, соответствующей области разрешенного сетевого взаимодействия, или нет. В случае обнаружения аномалии - признаков трафика, выходящих за пределы области разрешенного сетевого взаимодействия, можно утверждать, что обнаружена аномальная активность устройства, и оно используется не по назначению.

В силу ограниченной и неизменной функциональности устройства классификатор не требует регулярных обновлений в отличии, например, от базы сигнатур сетевой системы обнаружения вторжений (HIDS). Также, несомненным преимуществом такого решения в условиях дефицита ресурсов устройств является стабильно низкий уровень потребления ресурсов для хранения и функционирования классификатора в рабочем состоянии на протяжении всего времени эксплуатации устройства. Объем затрачиваемых устройством ресурсов на хранение классификатора зависит от представления области разрешенного сетевого взаимодействия и выбранной технологии построения классификатора.

Например, если классификатор построен на основе нейронной сети, обученной на признаках сетевого трафика из области разрешенного сетевого взаимодействия, полученных без инспекции содержимого сетевого трафика, то для расчета таких признаков в режиме реального времени и их анализа классификатором, а также для хранения на устройстве настроенной нейронной сети, которая представляет собой числовую матрицу весов составляющих ее нейронов, значительные ресурсы не требуются.

Признаки, входящие в область разрешенного сетевого взаимодействия, могут рассчитываться на основе:

- используемых устройством сетевых портах и протоколах при реализации своих прикладных функций,
- статистики сетевого трафика и направлений открытия соединений при реализации устройством своих прикладных функций,
- данных о потреблении ресурсов процессора и памяти при реализации устройством ограниченной функциональности своих прикладных функций и др.

Выбранные признаки должны удовлетворять следующему условию. Значения признаков, получаемые при несанкционированном использовании устройства и/или генерации им атакующего трафика вовне, должны отличаться от значений признаков, получаемых при использовании устройства по назначению.

Признаки, участвующие в классификации, рассчитываться на основе тех же данных, но уже в процессе эксплуатации устройства в рабочем режиме, когда неизвестно, используется устройство по назначению или нет. А классификатор, заранее настроенный на признаках, входящих в область разрешенного сетевого взаимодействия, должен обладать возможностью относить набор признаков, поданный на его вход в текущий момент времени при эксплуатации устройства в рабочем режиме, к нормальному или аномальному.

Например, известный перечень сетевых протоколов и направлений открытия соединений при нормальном функционировании легко позволит выявить распределенную атаку типа DDoS с использованием незнакомых протоколов. Возможен

также несложный анализ пакетов данных, например, с использованием регулярных выражений, позволяющий отличить нормальные пакеты протокола от незнакомых, а значит, потенциально относящихся к атакующему трафику.

Однако методы, используемые для построения классификатора, могут быть различными: от систем формальных правил, сигнатурных и статистических методов до методов машинного обучения, включая решающие деревья, искусственные нейронные сети, а также их комбинаций. Классификатор должен быть обучен распознавать один класс образов - соответствующий нормальной активности устройства, не распознанные классификатором образы считаются аномальными.

Классификатор может быть реализован как с помощью нейросетевого одноклассового классификатора, так и с помощью одноклассового классификатора на основе одного из методов машинного обучения. При этом в режиме настройки по окончании обучения одноклассового классификатора вся база образов, соответствующих нормальной активности устройства, проверяется на обученном классификаторе для вычисления ошибки распознавания образа. Полученный средний уровень ошибки, скорректированный в соответствии с установками алгоритма обнаружения аномалий, может быть использован в качестве порога ошибки в критерии обнаружения аномалии. И тогда, для подаваемых в реальном времени на вход обученного классификатора образов, представляющих собой признаки или наборы признаков, рассчитанные по данным текущего входного и выходного трафика, классификатором может быть рассчитана ошибка распознавания образов. В случае если для некого образа ошибка превышает установленный порог, то этот образ, характеризующий сетевую активность устройства в данный момент времени, признается аномальным.

Построение области разрешенного сетевого взаимодействия и классификатора для конкретного сетевого устройства ограниченной функциональности может выглядеть сложной задачей, требующей трудоемкого анализа спецификаций. В связи с этим задача построения такого классификатора является вполне выполнимой для производителя устройств ограниченной функциональности, поскольку в компактном виде отражает спецификации на продукт. Поэтому подобный классификатор может быть построен с помощью методов машинного обучения на основе сетевого трафика устройства, полученного в процессе очередного этапа производства - релизного тестирования, когда тестируются все штатные функции устройства. Такой классификатор должен встраиваться в ПО устройства в целях независимого контроля за входящим и исходящим сетевым трафиком и обнаружения аномалий в работе устройства.

Идентичность серийных устройств с одним и тем же ПО обеспечивает тиражируемость разработанного классификатора, то есть исключает необходимость построения классифицирующего модуля индивидуально для каждого сетевого устройства ограниченной функциональности. Однако, при обновлении ПО с корректировкой функциональности устройства, что не характерно для устройств такого типа, может возникнуть необходимость в актуализации классификатора.

Для осуществления способа устройства должны обладать возможностью отправлять защищенные от подмены сообщения (далее сообщения) при обнаружении собственной аномальной активности на единый сетевой узел - шлюз, который ретранслирует полученные сообщения в модуль анализа шлюза. При этом каждое сообщение содержит сетевой адрес устройства, на котором зафиксирована аномалия. Эти функции выполняет коммуникационный модуль, принимающий сигналы об обнаружении аномалии от классифицирующего модуля, формирующий и передающий соответствующие сообщения

на шлюз в реальном режиме времени.

Учитывая, что данное сообщение является предупреждением об обнаружении потенциального источника атаки с указанием его сетевого адреса, а сетевые устройства ограниченной функциональности уязвимы, не исключены попытки изменения сообщений злоумышленником или вывода из строя модулей их формирования. Поскольку сообщения должны быть отправлены на шлюз без задержек, крайне важно обеспечить защиту классифицирующего и коммуникационного модуля от взлома и отключения и защиту сообщений от подмены на этапе формирования и передачи по сети. Для этого целесообразно реализовать модуль обнаружения аномалий, в состав которого входят классифицирующий и коммуникационный модули, на уровне самых защищенных компонентов ОС или с использованием технологий доверенного вычислительного окружения, таких как, например, ARM TrustZone. Для обеспечения защиты сообщения от подмены и возможности получателю - модулю анализа шлюза, проверить достоверность и подлинность сообщения и его источника - устройства, должен быть использован один из современных и надежных методов аутентификации сообщений, например, Public Key Infrastructure (PKI).

Таким образом, при получении от классификатора сигнала об обнаружении аномалии в активности сетевого устройства коммуникационный модуль в реальном времени формирует защищенное от подмены сообщение, которое содержит сетевой адрес данного устройства, и отправляет его на установленный адрес шлюза.

Для удобства реализации и широкого использования способа важно, чтобы защищенные от подмены сообщения, формируемые коммуникационными модулями устройств, были унифицированы, то есть имели единообразный формат даже для устройств различного прикладного назначения и производителя. Целесообразно в перспективе разработать для этого стандарт.

Обман модуля обнаружений аномалий возможен в том случае, если программа агента ботнета сможет замаскировать свой трафик под нормальный. Однако, такая маскировка требует знания правил классификатора для конкретного устройства. Адаптация программ ботнета под широкий спектр устройств делает задачу создания ботнета слишком сложной и нецелесообразной.

Обнаружение аномалии в сетевом трафике устройства может быть ложным срабатыванием, поэтому модуль обнаружения аномалий не должен препятствовать функционированию устройства, в которое он встроен. Однако, если сообщения, отправляемые при обнаружении аномалий коммуникационными модулями устройств, объединенных в сеть, будут обрабатываться на стороне шлюза, который обеспечивает им выход в Интернет, то становится возможным определить, сообщения об аномалиях на отдельных устройствах приходят в случайные моменты времени или одновременно, что является признаком несанкционированного использования устройств в целях организации распределенной атаки. Поэтому на стороне шлюза необходимо создание агрегирующего модуля - модуля анализа, способного обрабатывать сообщения и выявлять корреляцию поступающих от множества устройств сообщений. Поскольку коммуникационные модули в своих сообщениях раскрывают сетевой адрес своего устройства, то при получении модулем анализа множества одновременных сообщений об аномалии и несложного анализа сетевого трафика, связанного только с раскрытыми сетевыми адресами, можно обнаружить признаки исходящей распределенной атаки, для предотвращения которой достаточно сформировать и применить правила фильтрации трафика.

В связи с этим для использования способа необходимо установить шлюз на границе

локальной и глобальной сети, который должен предоставлять устройствам, имеющим встроенный модуль обнаружения аномалий и объединенным в одну локальную сеть, доступ к глобальной сети и обладать возможностью фильтровать проходящий через него трафик по получаемым правилам, а также иметь в своем составе модуль анализа сетевой активности устройств локальной сети. Причем шлюз и модуль анализа должны иметь возможность обмениваться информацией. Шлюз должен обладать возможностью передавать модулю анализа сообщения, получаемые от коммуникационных модулей устройств, предоставлять данные о доступных сетевых адресах в его локальной сети, о сетевом трафике по запросу модуля анализа и принимать от модуля анализа правила фильтрации.

При этом модуль анализа должен быть выполнен с возможностью:

- приема и обработки защищенных от подмены сообщений от сетевых устройств ограниченной функциональности,
- запроса, приема и анализа сетевого трафика устройств ограниченной функциональности,
- предустановки признаков исходящей распределенной сетевой атаки;
- формирования правил фильтрации на основе анализа и их отправки на шлюз.

Модуль анализа может быть выполнен в виде программного средства и встроен в шлюз, также представляется возможным реализовать модуль анализа как автономное программно-аппаратное устройство. В случае реализации модуля анализа в программном виде формирование его может выполнить специалист по программированию (программист) на основе известных выполняемых функций.

Модуль анализа выполняет функции обнаружения несанкционированного использования устройств из сети, запрашивает у шлюза и анализирует сетевой трафик устройств в случае обнаружения их несанкционированного использования для поиска признаков исходящей распределенной атаки и формирования правил фильтрации для ее предотвращения, которые впоследствии отправляются и выполняются на шлюзе.

Для того, чтобы принимать решения о несанкционированном использовании устройств и об их участии в распределенной атаке, модуль анализа должен быть выполнен с возможностью получать и обрабатывать сообщения от устройств в реальном времени, а также проверять предварительно заданное в нем условие несанкционированного использования устройств.

Для этого в модуле анализа должны быть реализованы функции приема сообщений и средства их обработки, включая функции проверки аутентичности получаемых от устройств сообщений, вычисления параметра их взаимосвязи и чтения.

Также в модуле анализа должны быть заложены два режима функционирования: режим настройки и рабочий режим. В режиме настройки производится как первичная установка количества устройств в локальной сети, допустимого уровня аномальной активности, расчет порогового значения для условия обнаружения несанкционированного использования устройств и предустановка признаков обнаружения исходящей распределенной сетевой атаки, так и перенастройка в случае изменения состава локальной сети. В рабочем режиме модуль анализа функционирует с зафиксированными параметрами настроек, предустановленными условием обнаружения несанкционированного использования и признаками обнаружения исходящей распределенной сетевой атаки.

В режиме настройки модуль анализа шлюза настраивается для применения в конкретной локальной сети, а именно, определяется количество сетевых устройств ограниченной функциональности, находящихся в локальной сети, и допустимый для

данной локальной сети уровень аномальной активности. Это легко осуществимо благодаря возможности шлюза определять доступные сетевые адреса устройств, находящихся в локальной сети, и передавать информацию об уникальных действующих сетевых адресах модулю анализа. Из полученной информации модулем анализа может быть определено актуальное количество устройств в локальной сети. Данные о количестве устройств в сети и допустимом уровне аномальной активности будут использоваться модулем анализа для формирования условия обнаружения несанкционированного использования устройств.

Под допустимым уровнем аномальной активности в локальной сети понимается, тот уровень аномальных событий в сети, который еще считается допустимым и нормальным, но превышение которого будет признаком нарушения безопасности, возможной сетевой атаки на устройства в локальной сети, их несанкционированного использования или осуществления распределенной атаки с их помощью.

Допустимый уровень аномальной активности выражается в процентах и рассчитывается как доля устройств, на которых была одновременно зафиксирована аномальная активность, выявленная в результате работы модулей обнаружения аномалий, установленных на устройствах, относительно общего количества устройств локальной сети. Существование такого уровня обусловлено тем, что практически всем алгоритмам обнаружения аномалий характерно то или иное количество ложных срабатываний - обнаружения аномалий, когда устройство на самом деле используется по назначению.

На основе значения допустимого уровня аномальной активности модулем анализа рассчитывается пороговое значение для условия обнаружения несанкционированного использования устройств, превышение которого будет являться нарушением безопасности и означать обнаружение несанкционированного использования устройств.

Выбор допустимого уровня аномальной активности для конкретной локальной сети обусловлен количеством устройств, находящихся в локальной сети, и особенностями их функционирования в рабочем режиме, характеризующиеся возможными ложными срабатывания встроенного алгоритма обнаружения аномалий.

В рабочем режиме устройства не только выполняют свои прикладные функции, но и в режиме реального времени отправляют специальным образом сформированные сообщения при обнаружении своей аномальной активности.

Допустимый уровень аномальной активности может быть определен несколькими способами.

Допустимый уровень аномальной активности может быть определен модулем анализа в режиме настройки, в котором модуль анализа фиксирует максимальное количество одновременно получаемых аутентичных сообщений от функционирующих в рабочем режиме устройств на протяжении, например, одной недели, охватывающей особенности функционирования устройств на протяжении недельного цикла. Под одновременностью в данном случае понимается определенный временной интервал, например, 1 секунда. Далее модуль анализа рассчитывает допустимый уровень аномальной активности как отношение максимального количества одновременно полученных аутентичных сообщений от устройств в секунду к количеству устройств в сети, умноженное на 100%. При этом есть верхняя граница допустимого уровня аномальной активности равная 10% при количестве устройств в сети более 10.

В другом способе определения допустимого уровня аномальной активности модулем анализа может быть использован режим настройки, в котором модуль анализа фиксирует максимальное количество одновременно получаемых аутентичных сообщений от

функционирующих в рабочем режиме устройств на протяжении, например, недели. После чего модуль анализирует трафик устройств, которые одновременно сообщали об аномальной активности, и, в случае, если по предустановленным признакам обнаружения распределенных атак определено, что на самом деле устройства не генерируют атакующий трафик, то рассчитывается уровень аномальной активности, признается допустимым для данной сети и устанавливается в настройках модуля анализа.

В целях снижения ошибок первого рода появляющихся при использовании предустановленного допустимого уровня аномальной активности и определенного на его основе условия обнаружения несанкционированного использования устройств, когда обнаружение несанкционированного использования устройств происходит, но признаков распределенной атаки нет, рекомендуется проводить дополнительный этап настройки. На дополнительном этапе период наблюдения может быть увеличен. После чего модулем анализа допустимый уровень аномальной активности для данной сети может быть скорректирован.

Также на период настройки может быть привлечен специалист по информационной безопасности, контролирующий события в локальной сети и позволяющий модулю анализа определить допустимый уровень аномальной активности в отсутствии реальных атак.

В еще одном способе допустимый уровень аномальной активности может быть определен исходя из предоставляемых разработчиком сведений, приложенных к «паспорту» устройства и содержащих результаты тестирования модуля обнаружения аномалий, внедренного в то или иное устройство. Исходя из информации о статистике ложных срабатываний модулей обнаружения аномалий, установленных на всех устройствах контролируемой локальной сети, можно оценить допустимый для нее уровень аномальной активности.

Кроме того, допустимый уровень аномальной активности для конкретной локальной сети может быть выбран экспертом исходя из знаний о количестве устройств в локальной сети и их функционировании в рабочем режиме, но не должен превышать 10% при количестве устройств в сети более 10.

Условие несанкционированного использования устройств носит пороговый характер. Такой выбор обусловлен тем, что возникновение одиночных во времени аномальных событий в локальной сети может быть вызвано как программными, аппаратными или системными сбоями, так и ложными срабатываниями встроенного в устройства алгоритма обнаружения аномалий, но множество одновременных сообщений об аномальной активности от устройств из локальной сети с большой долей вероятности не случайность, а признак их несанкционированного использования в целях организации распределенной атаки.

Введем понятие взаимосвязи получаемых модулем анализа сообщений. Одновременное поступление множества сообщений об аномальной активности указывает на взаимосвязь аномальных событий в локальной сети, чем выше степень взаимосвязи получаемых модулем анализа шлюза сообщений, тем больше вероятность нарушения безопасности.

С учетом этих соображений должно быть установлено пороговое значение параметра, характеризующего взаимосвязь получаемых модулем анализа сообщений, превышение которого будет означать обнаружение несанкционированного использования устройств, одновременно отправивших сообщения об аномальной активности. Параметр, характеризующий взаимосвязь, вычисляется в модуле анализа как количество поступающих в определенный интервал времени, например, за 1 секунду, аутентичных

сообщений от устройств, обнаруживших свою аномальную активность. Пороговое значение этого параметра определяется в зависимости от общего количества устройств, находящихся в локальной сети, и допустимого уровня аномальной активности.

Например, пусть в локальной сети находится 300 устройств, при этом установленный допустимый уровень аномальной активности - 10%. В таком случае, пороговое значение параметра, характеризующего взаимосвязь получаемых модулем анализа сообщений, составляет $\frac{300\%\times10}{100\%}$=30. На основе этого значения модуль анализа определяет условие обнаружения несанкционированного использования устройств. В данном случае условие обнаружения несанкционированного использования устройств будет выполнено, когда параметр, характеризующий взаимосвязь полученных сообщений, рассчитываемый модулем анализа каждый раз по истечении определенного интервала времени - ежесекундно, превысит установленное пороговое значение. Это будет означать, что на модуль анализа шлюза за 1 секунду поступило более 30 сообщений, прошедших процедуру аутентификации, от устройств, обнаруживших свою аномальную активность. Именно для этих устройств модулем анализа будет сделан вывод об их несанкционированном использовании. Сетевые адреса данных устройств, которые могут быть прочитаны модулем анализа из полученных сообщений, должны быть занесены в список устройств, для которых сделан вывод об их несанкционированном использовании.

Определенный интервал времени, за который модулем анализа будет подсчитываться количество поступивших сообщений, принят равным 1 секунде. Однако, интервал может быть изменен в целях повышения уровня безопасности, с учетом таких факторов, как скорость обработки сетевых запросов устройствами, существенно ограниченными в ресурсах, с одной стороны, и возможность постепенного заражения устройств и отправки команд от командного центра на устройства с определенной задержкой, с другой стороны.

Также в модуле анализа могут быть установлены модифицированные правила расчета параметра, взаимосвязи между получаемыми от устройств сообщениями об аномальной активности, которые бы позволяли фиксировать зависимость между происходящими в сети аномальными событиями на некоторой предыстории, что особенно важно для обнаружения распределенного во времени несанкционированного использования устройств, направленных на них или исходящих от них распределенных во времени атак.

Важно отметить, что при изменении состава локальной сети, при подключении новых устройств или при отключении устройств от сети, информация о количестве устройств в локальной сети и допустимом уровне аномальной активности должна быть автоматически обновлена в модуле анализа, это необходимо для обновления условия несанкционированного использования устройств. Это обеспечивается за счет возможности шлюза предоставлять модулю анализа данные о доступных сетевых адресах в его локальной сети. При получении этой информации модулем анализа может быть определено актуальное количество устройств и скорректирован допустимый уровень аномальной активности.

Для определения факта исходящей распределенной атаки модуль должен обладать возможностью анализировать сетевую активность устройств, адреса которых занесены в список несанкционированно использующихся, а именно, осуществлять поиск признаков распределенной атаки в их сетевом трафике. Это осуществимо благодаря возможности шлюза ретранслировать модулю анализа сетевой трафик.

В рабочем режиме модуль анализа при обнаружении несанкционированного использования некоторого множества устройств должен запросить и принять сетевой трафик от шлюза для анализа сетевой активности устройств.

При этом необходимо отметить разницу между сетевым трафиком и сетевой активностью устройств. Сетевой трафик устройств локальной сети - это объем информации, измеряемый количеством бит или пакетов и передаваемый между устройствами локальной сети и шлюзом за определенный период времени.

Модуль анализа запрашивает у шлюза сетевой трафик, связанный только с сетевыми адресами из списка, то есть сетевой трафик тех устройств, для которых выполнено условие обнаружения несанкционированного использования, и выявляет в нем общие для всех устройств и характерные для исходящей распределенной атаки признаки. Например, если устройства, трафик которых анализируется, пытаются открывать сетевые соединения с узлом в глобальной сети или пытаются отправить большое число пакетов определенного типа на один сетевой адрес, который раньше не использовался, или вдруг стали осуществлять длительную отправку тел сообщений, или объем генерируемого каждым устройством трафика приближается к верхней границе их полосы пропускания и направлен на один сетевой адрес, то такая сетевая активность явно свидетельствует об исходящей от устройств распределенной атаке.

Таким образом, основным признаком распределенной атаки в трафике, исходящем от сетевых адресов из списка, является одинаковый адрес назначения отправляемых пакетов, отличный от используемых ранее. Признаками исходящей распределенной атаки также могут быть одинаковые протоколы, флаги, размеры сообщений, отправляемых на один сетевой адрес в глобальной сети, одинаковые и массовые запросы на подключение к одному сетевому адресу в глобальной сети, одинаковые HTTP-запросы и т.д. Например, когда все устройства отправляют TCP пакеты с SYN флагом или UDP, ICMP пакеты, при этом пакеты отправляются с большой скоростью, это явным образом говорит об обнаружении атак типа SYN Flood или UDP Flood, ICMP Flood.

Для поиска таких признаков и их совокупностей модуль анализа проводит сравнительный анализ ключевых полей пакетов, передаваемых устройствами с сетевыми адресами из списка, и ищет совпадения, а также может измерять основные характеристики трафика. Наличие таких признаков в сетевом трафике устройств, сообщивших о своей аномальной активности и для которых было выполнено условие обнаружения несанкционированного использования, говорит об обнаружении исходящей от них распределенной сетевой атаки, направленной на один сетевой узел глобальной сети. Признаки распределенной атаки должны быть заранее предустановлены в модуле анализа шлюза.

В случае обнаружения признаков распределенной атаки в сетевом трафике, модуль анализа инициирует упреждающие действия, формируя и отправляя на шлюз правила фильтрации, запрещающие атакующему трафику выход в глобальную сеть. При этом правила фильтрации формируются на основе обнаруженных признаков. В общем случае, правила фильтрации могут использовать любые данные заголовков IP (IP-адреса источника и получателя). Например, если было обнаружено, что все сетевые адреса из списка отправляют одинаковые пакеты TCP с SYN флагом на один IP-адрес, то правила фильтрации будут сформированы таким образом, чтобы заблокировать сетевые пакеты, направленные на данный IP-адрес. После того, как созданные правила фильтрации будут предоставлены сетевому шлюзу от модуля анализа и применены, распределенная атака будет предотвращена до ее выхода в глобальную сеть.

Поскольку каждое устройство из локальной сети в рабочем режиме при обнаружении

собственной аномальной активности специальным образом формирует сообщение, содержащее собственный сетевой адрес, и модуль анализа обрабатывает сообщения только в случае выполнения условия обнаружения несанкционированного использования устройств и процедур аутентификации, то необходимо проанализировать только ограниченное количество трафика, источником которого являются сетевые адреса, указанные в сообщениях. Такая особенность способа существенно сужает выборку необходимого для анализа сетевого трафика и упрощает последующее составление правил фильтрации, обеспечивая сокращение затрачиваемых модулем анализа ресурсов для обнаружения и предотвращения распределенных атак.

Таким образом, совместная работа сформированных классифицирующего и коммуникационного модуля в составе модуля обнаружения аномалий на базе каждого устройства из одной локальной сети и настроенного модуля анализа на базе шлюза, установленного на границе локальной и глобальной сети, обеспечивает обнаружение несанкционированного использования устройств, обнаружение и предотвращение распределенных атак, исходящих от устройств локальной сети, и выглядит следующим образом.

При запуске устройств в рабочем режиме в каждом встроенном классифицирующем модуле в режиме реального времени по данным входящего и исходящего трафика рассчитываются признаки, характеризующие текущую активность устройства. Признаки в формате, зависящем от выбранного классификатора, подаются на вход классификатора, обученного на множестве признаков сетевого трафика, описывающем область разрешенного сетевого взаимодействия устройства. Классификатор по заданному алгоритму определяет считать ли текущую активность устройства нормальной или аномалий. Алгоритм может состоять в простом сравнении полученных признаков с признаками из области разрешенного взаимодействия, например, в сравнении используемых протоколов, портов с установленными в классификаторе. При этом в случае несоответствия классифицирующий модуль в режиме реального времени передает сигнал об аномалии на вход коммуникационного модуля.

В другом варианте в классификаторе, реализованном в виде нейронной сети, может быть настроен порог ошибки распознавания входного образа признаков, при превышении которого генерируется сигнал об обнаружении аномалии и передается на коммуникационный модуль.

Коммуникационный модуль, также встроенный в ПО устройства, обладает возможностью отправлять специальным образом сформированные защищенные от подмены сообщения на адрес шлюза, который ретранслирует сообщения модулю анализа. Модуль анализа в реальном времени проверяет полученные сообщения на аутентичность и, отбрасывая неаутентичные, вычисляет параметр, характеризующий взаимосвязь полученных аутентичных сообщений, как количество поступающих сообщений за определенный интервал времени, равный 1 секунде. Каждый раз по истечении определенного интервала времени модулем анализа выполняется проверка предустановленного условия обнаружения несанкционированного использования устройств, основанного на пороговом значении для параметра, характеризующего взаимосвязь полученных сообщений.

Если условие обнаружения несанкционированного использования устройств не выполнено, то модуль анализа возвращается к этапу проверки аутентичности защищенных от подмены сообщений, приходящих от устройств.

При выполнении условия обнаружения несанкционированного использования устройств модуль анализа фиксирует полученные за определенный интервал времени,

равный 1 секунде, сообщения, извлекает сетевые адреса из сообщений и заносит их в список адресов устройств, для которых сделан вывод об их несанкционированном использовании. Таким образом, каждым устройством локальной сети может быть обнаружена собственная аномальная активность, а множество аномальных событий в сети, то есть несанкционированное использование множества устройств из локальной сети, может быть обнаружено модулем анализа, принимающим сообщения от всех устройств локальной сети.

После чего модуль анализа запрашивает у шлюза сетевой трафик перечисленных в списке сетевых адресов. В полученном сетевом трафике модуль анализа проводит поиск таких признаков распределенной атаки, как множественные попытки всех устройств открыть сетевое соединение с одним узлом в глобальной сети, выполнить однотипные запросы к одному сетевому ресурсу, отправить большое число пакетов определенного типа на один сетевой узел в глобальной сети и др. При обнаружении такой сетевой активности модулем анализа инициируется формирование правил фильтрации для этого сетевого трафика, цель которых состоит в блокировании выявленного при анализе атакующего трафика. После передачи правил фильтрации на шлюз они применяются до тех пор, пока в модуле анализа выполняется условие несанкционированного использования устройств, осуществляя тем самым предотвращение скоординированной распределенной атаки исходящей со стороны устройств локальной сети.

Поскольку корреляция аномальных событий подразумевает некоторый порог нечувствительности, когда рассчитываемое значение параметра, характеризующего взаимосвязь получаемых модулем анализа сообщений, ниже порогового, возможны случаи ошибок второго рода - часть атакующего трафика будет пропущена в Интернет. Однако, мощности таких атак будет недостаточно для того, чтобы вызвать «отказ в обслуживании» у атакуемого ресурса.

Стоит отметить, что посредством анализа трафика устройств, которые были не санкционированно использованы при попытке организации распределенной атаки, и это было обнаружено модулем анализа, можно выявить командный центр данного ботнета, если, как это часто бывает, ботнет централизованный. Это позволит не только впредь блокировать любые соединения с этим источником, но и обнародовать эти сведения для защиты других ресурсов.

Основным отличием заявляемого способа от известных является то, что обнаружение и предотвращение атаки происходит не на стороне "жертвы" распределенной атаки после обнаружения последствий атаки, а на стороне источника атаки - шлюза, и блокируется до выхода в Интернет, обеспечивая принципиальную невозможность достижения распределенной атакой своей цели и каких-либо серьезных последствий на атакуемом сетевом узле.

Преимуществом заявляемого способа является повышение эффективности, что проявляется в сокращении времени задержки обнаружения и предотвращения распределенных атак. Такой результат достигается за счет обнаружения несанкционированного использования сетевых устройств ограниченной функциональности в целях организации распределенных атак с их участием, а именно, признаков распределенных атак в сетевом трафике устройств ограниченной функциональности, одновременно сообщивших об обнаружении собственной аномальной активности. То есть обнаружение исходящей распределенной атаки происходит на этапе формирования вредоносных пакетов, а предотвращение атаки осуществляется путем блокировки атакующего трафика до попадания вредоносных пакетов в глобальную сеть. Предлагаемый способ позволяет исключить недостаток

существующих методов обнаружения и предотвращения вторжений - задержку обнаружения и предотвращения атак, поскольку при обнаружении атаки путем выявления ее последствий на атакуемом ресурсе проходит больше времени с момента начала атаки, чем при обнаружении атаки в ее источнике.

Еще одним преимуществом способа является отсутствие высоких требований к аппаратным и вычислительным ресурсам для его эффективной реализации. Поскольку для осуществления способа достаточно тех ресурсов, которые могут быть предоставлены существующими устройствами ограниченной функциональности и шлюзом.

Другим преимуществом предложенного способа является то, что не требуется передача пользовательских данных в любой, даже анонимной форме, а также не требуется предоставления специального доступа к сетевым устройствам ограниченной функциональности со стороны шлюза.

Несмотря на то, что способ обеспечивает обнаружение несанкционированного использования только тех устройств, которые находятся в пределах контролируемой модулем анализа шлюза локальной сети, представляется возможным масштабировать предложенный способ. Например, за счет разработки средства для обмена данными о несанкционированном использовании устройств между модулями анализа на уровне Интернет-провайдера. Наличие агрегатора событий на верхних уровнях сетевой иерархии позволило бы выявлять и блокировать более масштабные распределенные атаки, исходящие от сетевых устройств ограниченной функциональности из различных географически распределенных локальных сетей. Важность такой возможности нельзя недооценивать, поскольку ботнеты - это сети зараженных устройств, расположенных в разных странах мира. Такой способ при широком использовании мог бы устранить крупномасштабную угрозу ботнетов, осуществляющих мощнейшие распределенные атаки, и решить проблему задержки обнаружения и предотвращения распределенных атак.

Осуществление изобретения

Рассмотрим осуществление предложенного способа в сети с коммутацией пакетов. Это может быть, например, корпоративная сеть, имеющая выход в сеть Интернет через один основной шлюз и включающая 100 IP-видеокамер одной модели с ОС на базе Linux, используемых в системе охраны и наблюдения офисного здания.

Поскольку такие IP-видеокамеры - это микрокомпьютеры с ОС, то в каждую IP-видеокамеру может быть встроен программный модуль обнаружения аномалий. Функционал IP-видеокамеры достаточно прост, поэтому область разрешенного сетевого взаимодействия может быть представлена списком сетевых адресов, типов протоколов, и номеров портов, использующихся для передачи данных в рамках основных функций камеры, а также максимальным уровнем потребления ресурсов процессора и памяти при реализации камерой своих прикладных функций. Классифицирующий модуль формируется на основе области разрешенного сетевого взаимодействия и пригоден для использования во всех IP-видеокамерах данной сети. Классифицирующий модуль выполняется таким образом, что при обнаружении использования IP-видеокамерой сетевого адреса, протокола или порта для передачи данных, отличного от указанных в списке разрешенных, или при превышении максимального уровня потребления ресурсов, генерируется сигнал аномалии. Коммуникационный модуль реализуется с возможностью приема сигналов об аномалии от классифицирующего модуля, формирования защищенных от подмены сообщений в едином формате, содержащих сетевой адрес камеры, и их отправки на прописываемый сетевой адрес используемого шлюза. Поскольку крайне важно избежать потери или подмены сообщений, необходимо

осуществлять операции по обнаружению аномальной активности и формированию сообщений на уровне защищенных компонентов ОС IP-видеокамер. Классифицирующий и коммуникационный модули объединяются в модуль обнаружения аномалий и внедряются в доверенное окружение IP-видеокамеры, защищенное от проникновения стороннего ПО. Такая возможность обеспечивается использованием технологии ARM TrustZone.

Таким образом, в ПО каждой IP-видеокамеры встраивается модуль обнаружения аномалий, выполненный как специализированная программа (СП), позволяющая обеспечить:

- выход в глобальную сеть через шлюз,
- обнаружение собственной аномальной активности,
- формирование и передачу модулю анализа шлюза защищенного от подмены сообщения, раскрывающего сетевой адрес IP-видеокамеры при обнаружении им собственной аномальной активности.

Все IP-видеокамеры находятся в одной локальной сети, на границе которой установлен шлюз. В качестве шлюза используется сетевой шлюз, поддерживающий функции фильтрации. В шлюз встраивается модуль анализа, выполненный в виде специализированного ПО, обеспечивающего возможность обмена данными между шлюзом и модулем анализа. Модуль анализа выполняется с возможностью:

- приема и обработки защищенных от подмены сообщений от IP-видеокамер,
- предустановки признаков исходящей распределенной сетевой атаки,
- запроса, приема и анализа сетевого трафика IP-видеокамер,
- формирования правил фильтрации на основе анализа и отправки их на шлюз.

Причем в качестве предустановленных признаков исходящей распределенной атаки установлен один признак: одинаковый IP-адрес назначения в сетевых пакетах, направляемых всеми IP-видеокамерами, трафик которых анализируется.

Для обеспечения защиты сообщений от подмены и обеспечения возможности получателю - модулю анализа шлюза, проверить достоверность и подлинность сообщения и его источника используется надежный метод аутентификации сообщений - PKI.

После развертывания в локальной сети IP-видеокамер, способных сообщать об обнаружении собственной аномальной активности, и установки шлюза с включенным в него модулем анализа можно приступить к использованию способа.

В модуле анализа шлюза устанавливается количество IP-видеокамер - 100 и допустимый уровень аномальной активности - 10%. В модуле анализа рассчитывается пороговое значение для условия обнаружения несанкционированного использования устройства по формуле: $\frac{10\% \times 100}{100\%} = 10.$ В модуле анализа условие обнаружения несанкционированного использования определяется как: P>10, где P - параметр, характеризующий взаимосвязь получаемых модулем анализа сообщений. Данный параметр рассчитывается как количество поступивших на модуль анализа аутентичных сообщений в течение выбранного интервала времени - 1 секунды.

IP-видеокамеры и шлюз запускаются в рабочем режиме. После запуска IP-видеокамер в случае обнаружения аномальной, нетипичной для выполнения своих прикладных функций активности в режиме реального времени ими генерируются защищенные от подмены сообщения и передаются на адрес шлюза. Шлюз ретранслирует сообщения модулю анализа.

В рабочем режиме модуль анализа проверяет полученные от IP-видеокамер сообщения на аутентичность и отбрасывает неаутентичные.

Каждую секунду модуль анализа рассчитывает количество полученных им аутентичных сообщений - параметр, характеризующий взаимосвязь между сообщениями, и проверяет условие несанкционированного использования устройств. Если параметр, характеризующий взаимосвязь полученных сообщений, окажется больше порогового значения, заданного в модуле анализа, то условие несанкционированного использования выполняется.

Допустим, за 1 секунду модуль анализа получил 15 аутентичных сообщений, тогда условие обнаружения несанкционированного использования выполняется. Модуль анализа фиксирует и обрабатывает полученные сообщения, извлекая сетевые адреса, которые раскрываются IP-видеокамерами в сообщениях. Модуль анализа записывает извлеченные сетевые адреса в список. Таким образом, составлен список сетевых адресов устройств, для которых выполнено условие и сделан вывод об их несанкционированном использовании.

Далее в реальном времени модуль анализа проверяет, вызвано ли несанкционированное использование IP-видеокамер, сетевые адреса которых перечислены в списке, попыткой использовать их в распределенной атаке. Для этого модуль анализа запрашивает у шлюза сетевой трафик, связанный с сетевыми адресами, перечисленными в списке, и осуществляет в нем поиск предустановленного признака исходящей распределенной атаки - одинакового адреса назначения в сетевых пакетах, отправляемых с 15 сетевых адресов, перечисленных в списке.

Если в результате сравнительного анализа найдены совпадения и определено, что все 15 IP-видеокамер отправляют пакеты на один IP-адрес, это означает, что обнаружена исходящая распределенная атака. Для предотвращения атаки модуль анализа формирует правила фильтрации сетевого трафика, запрещающие IP-видеокамерам, сетевые адреса которых перечислены в списке, передачу пакетов на выявленный в результате анализа трафика IP-адрес.

Правила фильтрации передаются модулем анализа на шлюз, где они принимаются и применяются. Шлюз фильтрует трафик до тех пор, пока в модуле анализа шлюза выполняется условие несанкционированного использования устройств. Таким образом, предотвращение скоординированной распределенной сетевой атаки со стороны IP-видеокамер, для которых определен факт их несанкционированного использования, осуществляется за счет фильтрации сетевого трафика IP-видеокамер из локальной сети с помощью шлюза согласно полученным от модуля анализа правилам фильтрации.

Модуль анализа, являющийся агрегатором аномальных событий локальной сети, позволяет обнаружить несанкционированное использование некоторых устройств из сети, проанализировать трафик этих устройств, и при обнаружении в нем признаков распределенных атак сформировать правила фильтрации, запрещающие атакующему трафику выход в Интернет, обеспечивая принципиальную невозможность достижения распределенной атакой ее цели.

Способ допускает реализацию описанных модулей в виде программной системы, функционирующей на существующих сетевых устройствах ограниченной функциональности и шлюзах.

Необходимо отметить, что возможны и другие варианты реализации предложенного способа, отличающиеся от описанного выше.

Источники информации, принятые во внимание при составлении заявки

1. Патент США №9661019, приоритет от 07.08.2014 г.

2. Патент КНР №107800727, приоритет от 12.12.2017 г..

3. Pamukchiev, A., Jouet, S., and Pezaros, D.P. “Distributed Network Anomaly Detection on

an Event Processing Framework”. In: IEEE Consumer Communications and Networking Conference 2017, Las Vegas, NV, USA, 8-11 Jan 2017.

4. Патент США №9167004, приоритет от 23.08.2012 г.

5. Vladimir Eliseev and Olga Eliseeva. “Lightweight Distributed Attack Detection and Prevention for the Safe Internet of Things”. Cyber Security 2018, June 11-12, 2018, Scotland, UK.

(57) Формула изобретения

1. Способ обнаружения несанкционированного использования сетевых устройств ограниченной функциональности из локальной сети и предотвращения исходящих от них распределенных сетевых атак на сетевые узлы в глобальной сети, при этом локальная сеть включает:

шлюз, установленный на границе локальной сети, содержащий модуль анализа и выполненный с возможностью

передачи трафика в ответ на запрос модуля анализа,

фильтрации трафика согласно принимаемым от модуля анализа правилам фильтрации;

сетевые устройства ограниченной функциональности, имеющие в своем составе операционную систему и выполненные с возможностью

выхода в глобальную сеть через шлюз,

обнаружения собственной аномальной активности,

формирования и передачи модулю анализа шлюза защищенного от подмены сообщения, раскрывающего сетевой адрес устройства ограниченной функциональности, при обнаружении им собственной аномальной активности;

причем модуль анализа выполнен с возможностью

предустановки признаков исходящей распределенной сетевой атаки,

приема и обработки защищенных от подмены сообщений от сетевых устройств ограниченной функциональности,

запроса, приема и анализа сетевого трафика устройств ограниченной функциональности,

формирования правил фильтрации на основе анализа и их отправки на шлюз;

тогда способ заключается в том, что

задают в модуле анализа количество сетевых устройств ограниченной функциональности в локальной сети и допустимый уровень аномальной активности в локальной сети;

определяют в модуле анализа условие несанкционированного использования сетевых устройств ограниченной функциональности;

запускают сетевые устройства ограниченной функциональности и шлюз в рабочем режиме;

получают в модуле анализа в режиме реального времени защищенные от подмены сообщения, содержащие сетевые адреса устройств ограниченной функциональности, обнаруживших свою аномальную активность; проверяют в модуле анализа полученные сообщения на аутентичность и отбрасывают неаутентичные;

вычисляют в режиме реального времени параметр, характеризующий взаимосвязь между полученными модулем анализа аутентичными сообщениями;

проверяют в модуле анализа выполнение условия несанкционированного использования сетевых устройств ограниченной функциональности;

если условие выполнено, то

выполняют в модуле анализа следующие действия:

формируют список сетевых адресов устройств ограниченной функциональности, для которых выполнено условие несанкционированного использования;

запрашивают у шлюза сетевой трафик устройств ограниченной функциональности, сетевые адреса которых перечислены в списке;

получают от шлюза сетевой трафик устройств ограниченной функциональности, сетевые адреса которых перечислены в списке;

анализируют сетевую активность посредством поиска в сетевом трафике устройств ограниченной функциональности, сетевые адреса которых перечислены в списке, признаков исходящей распределенной атаки;

формируют правила фильтрации сетевого трафика на основе анализа сетевой активности устройств ограниченной функциональности, сетевые адреса которых перечислены в списке; передают правила фильтрации на шлюз;

фильтруют сетевой трафик согласно полученным от модуля анализа правилам фильтрации с помощью шлюза, предотвращая скоординированную распределенную сетевую атаку со стороны сетевых устройств ограниченной функциональности, сетевые адреса которых перечислены в списке, до тех пор, пока в модуле анализа шлюза выполняется условие несанкционированного использования сетевых устройств ограниченной функциональности.

2. Способ обнаружения несанкционированного использования сетевых устройств ограниченной функциональности и предотвращения распределенных сетевых атак по п. 1, отличающийся тем, что защита сообщений, формируемых сетевыми устройствами ограниченной функциональности, от подмены обеспечивается за счет реализации операций определения аномальной активности и формирования сообщений на уровне защищенных компонентов операционной системы сетевого устройства ограниченной функциональности с использованием технологий доверенного вычислительного окружения.

3. Способ обнаружения несанкционированного использования сетевых устройств ограниченной функциональности и предотвращения распределенных сетевых атак по п. 1, отличающийся тем, что аутентификация сообщений, полученных модулем анализа от сетевых устройств ограниченной функциональности, осуществляется посредством применения инфраструктуры открытых ключей.

4. Способ обнаружения несанкционированного использования сетевых устройств ограниченной функциональности и предотвращения распределенных сетевых атак по п. 1, отличающийся тем, что защищенные от подмены сообщения, получаемые модулем анализа шлюза от сетевых устройств ограниченной функциональности, имеют единый формат для устройств различного прикладного назначения и производителя.

5. Способ обнаружения несанкционированного использования сетевых устройств ограниченной функциональности и предотвращения распределенных сетевых атак по п. 1, отличающийся тем, что условие несанкционированного использования сетевых устройств ограниченной функциональности является пороговым условием, в котором порог - это пороговое значение параметра, характеризующего взаимосвязь между получаемыми модулем анализа аутентичными сообщениями, зависящее от количества сетевых устройств в локальной сети и допустимого уровня аномальной активности для данной локальной сети.

6. Способ обнаружения несанкционированного использования сетевых устройств ограниченной функциональности и предотвращения распределенных сетевых атак по п. 5, отличающийся тем, что параметр, характеризующий взаимосвязь между

аутентичными сообщениями, полученными модулем анализа шлюза от сетевых устройств ограниченной функциональности, определяется количеством поступивших аутентичных сообщений за определенный интервал времени.

7. Способ обнаружения несанкционированного использования сетевых устройств ограниченной функциональности и предотвращения распределенных сетевых атак по п. 1, отличающийся тем, что в качестве признака исходящей распределенной атаки принимают отправку перечисленными в списке устройствами ограниченной функциональности пакетов на один сетевой узел глобальной сети.

8. Способ обнаружения несанкционированного использования сетевых устройств ограниченной функциональности и предотвращения распределенных сетевых атак по п. 7, отличающийся тем, что правила фильтрации запрещают перечисленным в списке устройствам ограниченной функциональности передачу пакетов сетевому узлу глобальной сети, определенному на этапе анализа сетевой активности при поиске признаков исходящей распределенной атаки.

9. Способ обнаружения несанкционированного использования сетевых устройств ограниченной функциональности и предотвращения распределенных сетевых атак по любому из пп. 1-8, отличающийся тем, что глобальная сеть представляет собой глобальную сеть Интернет, при этом шлюз установлен на стороне поставщика Интернет-услуг, который обеспечивает выход в Интернет сетевым устройствам ограниченной функциональности, образующим локальную сеть поставщика Интернет-услуг.

10. Способ обнаружения несанкционированного использования сетевых устройств ограниченной функциональности и предотвращения распределенных сетевых атак по любому из пп. 1-8, отличающийся тем, что при изменении количества сетевых устройств ограниченной функциональности в локальной сети информация о количестве сетевых устройств ограниченной функциональности и допустимом уровне аномальной активности в локальной сети должна быть обновлена в модуле анализа.