DOI 10.37882/2223-2966.2023.06.24

АНАЛИЗ ТРАФИКА ДАРКНЕТА ВРЕДОНОСНЫХ ПРОГРАММ IOT С ПОМОЩЬЮ АССОЦИАТИВНЫХ ПРАВИЛ

ANALYSIS OF IOT MALWARE DARKNET TRAFFIC USING ASSOCIATIVE RULES

A. Kulikov
Y. Kravtsova
A. Platoshin

Summary: This research paper examines the issues of cybersecurity in the context of the development of information technology and the Internet of Things (IoT — Internet of Things). Due to the increasing frequency of cyber-attacks in today's world, including the use of malicious software Mirai for IoT, it is necessary to develop mechanisms to detect cyber-attacks occurring on the Internet. Thus, the paper proposes the use of an anonymous network to detect cyber-attacks, as it is a system of virtual tunnels in which packets are generated by malware. Statistical methods and associative rule learning are used to analyze the behavior of scanning attacks based on the packets observed in the Darknet. Particular attention is paid to TCP SYN packets that characterize scanning attacks. The paper discusses the principles of anonymous networking, IP addresses, and the characteristics of the Mirai malware for IoT. The basic concepts used in finding associative rules, such as support and confidence, are also discussed, and the FP-Growth/FP-tree algorithm is proposed for finding such rules. A large set of TCP SYN packets collected by the NICT/16 Darknet sensor was used to evaluate the proposed method. The results show that the proposed method is efficient and can be used to find associative rules in large databases. The algorithm parameters and strategies for determining them to obtain the best results are also discussed. The research can be useful for developing new mechanisms for detecting cyber-attacks and improving cybersecurity.

Keywords: DarkNet, Cyberattacks, Mirai, analysis using associative rule learning, darknet, anonymous network, IoT.

Куликов Александр Анатольевич
К.т.н., доцент, РТУ МИРЭА, Москва, Россия
kulikov_aa@mirea.ru
Кравцова Екатерина Юрьевна
РТУ МИРЭА, Москва, Россия
9067320378@mail.ru
Платошин Александр Игоревич
РТУ МИРЭА, Москва, Россия
sasaplatosin@gmail.ru

Аннотация: Исследовательская работа рассматривает вопросы кибербезопасности в контексте развития информационных технологий и интернета вещей (англ. IoT — Internet of Things). В связи с участившимися кибератаками в современном мире, в том числе с использованием вредоносного программного обеспечения Mirai для IoT, необходимо разработать механизмы, позволяющие обнаруживать кибератаки, происходящие в Интернете. Таким образом, в статье предлагается использовать анонимную сеть для обнаружения кибератак, так как она представляет собой систему виртуальных туннелей, в которой пакеты генерируются вредоносными программами. Для анализа поведения сканирующих атак на основе пакетов, наблюдаемых в Даркнете, используются статистические методы и обучение по ассоциативным правилам. Особое внимание уделяется пакетам TCP SYN, характеризующим атаки сканирования. В статье рассматриваются принципы работы анонимной сети, IP-адреса, а также характеристики вредоносного ПО Mirai для IoT. Также рассматриваются основные понятия, используемые при поиске ассоциативных правил, такие как поддержка (support) и достоверность (confidence), а также предлагается использовать алгоритм FP-Growth/FP-tree для поиска таких правил. Для оценки предложенного метода использовался большой набор пакетов TCP SYN, собранных с помощью датчика Даркнета NICT/16. Результаты показали, что предложенный метод эффективен и может быть использован для поиска ассоциативных правил в больших базах данных. Также обсуждаются параметры алгоритма и стратегии их определения для получения наилучших результатов. Исследование может быть полезно для разработки новых механизмов обнаружения кибератак и повышения уровня кибербезопасности.

Ключевые слова: Даркнет, кибератаки, Mirai, анализ с использованием обучения по ассоциативным правилам, темная сеть, анонимная сеть, IoT.

Введение

Актуальность темы защиты входящего и выходящего трафика в сети обусловлена растущим числом устройств Интернета вещей (используется стандартное сокращение IoT) и их потенциальной уязвимостью перед кибератаками. Даркнет (англ. DarkNet) — является скрытой и анонимной сетью, внутри которой устанавливаются соединения только между доверенными пирами, используя нестандартные протоколы и порты. Анонимная сеть является системой не связанных между собой виртуальных туннелей, которые предоставляют передачу данных в зашифрованном виде. Главным отличием данной сети от других распределённых одноранговых сетей является то, что файлообмен происходит анонимно (поскольку IP-адреса недоступны публично), и поэтому пользователи могут общаться без опаски и риска государственного вмешательства. Из—за этого данная сеть часто выступает в роли инструмента для осуществления коммуникации в различные рода подпольях и незаконной деятельности. Термин «анонимная сеть» может иметь более широкое значение, включая описание некоммерческих узлов в интернете, а также относиться к технологиям и коммуникациям в Интернете, которые, в основном, связаны с незаконными действиями или выражением несогласия.

Данная анонимная сеть способствует распространению вредоносных программ, которые атакуют устройства Интернета вещей (англ. Internet of Things) повреждая данные пользователей нанося значительный ущерб. Анализ трафика сети с помощью ассоциативных правил позволяет обнаружить новые типы вредоносных программ и выявить связи между ними, для принятия мер защиты устройств Интернета вещей и данных пользователей. В целом, использование ассоциативных правил для анализа трафика анонимной сети является эффективным способом борьбы с киберугрозами в сфере IoT.

Материалы и методы

Описана работа правил ARL (англ. ARL —метод машинного обучения, в основе которого лежат правила обнаружения связей между переменными в большой базе данных). Использованы алгоритмы нахождения правил в значениях (itemsets) FP-Growth/FP-tree (англ. Frequent Pattern-Growth/Frequent-Pattern Tree). Произведена работа с пакетами TCP (англ. Transmission Control Protocol) и SYN (англ. Synchronize Sequence Numbers).

Литературный обзор

На сегодняшний день, «Вредоносные программы (ВП) совершенствуются с опережением антивирусных средств (АВС), поэтому требуется разработка технологий защиты информационных систем (ИС) с опережением над средствами нападения. Угрозы от ВП растут [1–3]. Известно множество ВП, они изучаются, классифицируются, формируются базы данных, прогнозируется их развитие и возможный ущерб» [1, с. 50].

Стоит отметить, «Главным преимуществом для тех, кто предпочитает Даркнет (по разным оценкам их число варьируется от 0,1 % до 1 % от всех пользователей интернета), выступает сохранение анонимности пользователей. В техническом отношении такая анонимность достигается за счет использования специальных браузеров TOR (луковых маршрутизаторов), которые не позволяют определить IP-адреса с помощью специальных способов шифрования и туннельной передачи данных. Информация в Даркнете передается в одноранговых сетях без возможности их контроля и перехвата [Biddle, England, Peinado, Willman 2003: 25]» [2, с. 12].

А также, «Хотя устройства Интернета вещей (IoTD) приносят пользу во многих аспектах жизни, эти устройства также создают риски безопасности в виде уязвимостей, которые дают хакерам миллиарды новых многообещающих целей. Например, ботнеты использовали недостатки безопасности, характерные для IoTD, для получения несанкционированного контроля над сотнями тысяч хостов, которые затем использовали для проведения массовых разрушительных распределенных атак типа «отказ в обслуживании» [3, с. 9].

Сам «Ботнет Mirai состоит из четырех основных компонентов. Бот — вредонос, заражающий устройства и распространяющий «инфекцию» среди неверно сконфигурированных устройств, а потом атакующий сервер-мишень при получении соответствующей команды от ботмастера — человека, управляющего ботами. Управляющий сервер предоставляет ботмастеру интерфейс, позволяющий проверять состояние ботнета и инициировать новые DDoS-атаки» [4, с. 12].

Принимая во внимание, что «Значение аббревиатуры DDoS происходит от английских слов distributed denial of service, что в переводе на русский язык означает прекращение доступа в обслуживание. Если разбирать досконально, то такая DDoS-атака направлена на вычислительную систему с определенной целью, которая в большинстве случаев заключается в выведении ее из строя или работоспособного состояния» [5, с. 227].

Результаты

Информационные технологии (ИТ) стремительно изменяются с течением времени. Огромное количество людей пользуется новыми преимуществами благодаря цифровым технологиям. В последние годы, в дополнение к этой революции в области ИТ, произошел прогресс в области Интернета вещей (англ. IoT), где различные вычислительные устройства, подключенные к беспроводной сети, способны собирать и передавать данные по ней исключая человеческое участие. Однако, вместе с развитием ИТ и IoT систем, участились кибератаки, использующие новые уязвимости системы, создавая серьезные проблемы в наши дни. В частности, огромное влияние оказало недавнее вредоносное программное обеспечение (ПО) Mirai для IoT.

Mirai — это вредоносная программа типа «Червь» (англ. Worm). Данный тип вредоносного ПО способен копировать себя и распространять по сети, используя уязвимости в системе безопасности. В случае с IoT-устройствами Mirai производила поиск с аналогичной уязвимостью для самовоспроизведения. Злоумышленник манипулирует зараженными IoT-устройствами, как ботами, для проведения распределенной атаки типа «отказ в обслуживании» (англ. DDoS) путем передачи большого количества пакетов на целевые узлы.

Для того, чтобы оперативно справиться с такой крупномасштабной интеллектуальной кибератакой, необходимо сконструировать механизм, способный наблюдать за кибератаками, происходящими в Интернете.

Неиспользуемое адресное пространство анонимной сети является системой виртуальных туннелей, причем не связанных между собой. Считается, что коммуникации между ними не происходит, поскольку в анонимной

сети нет ни одного устройства, но в действительности в систему поступает множество пакетов. Эти пакеты в основном вызваны активностью сканирования или обратным рассеянием ответных пакетов от целевых хостов, на которые направлена DDoS-атака. Именно поэтому можно считать, что пакет, наблюдаемый в анонимной сети, генерируется вредоносными программами. Таким образом, благодаря анализу пакетов анонимной сети можно обнаружить часть кибератак в Интернете.

В данном исследовании производится анализ поведения сканирующих атак на основе пакетов, наблюдаемых в Даркнете. Для анализа будут взяты пакеты TCP SYN, характеризующие атаки сканирования. Производится поиск статистических особенностей в TCP-заголовках этих пакетов, используя обучение по ассоциативным правилам к SYN-пакетам.

Анонимная сеть пользуется доступным пространством, использующим IP-адреса в Интернете. IP-адрес — это уникальный адрес, идентифицирующий устройство в интернете или локальной сети, выражается в виде 32-битных данных. Таким образом существует около 4,3 миллиарда IP-адресов. Однако не все из них назначаются хост-компьютерами. На самом деле, поступает значительное количество пакетов, хотя передача пакетов на неиспользуемый IP-адрес не происходит при обычном подключении к Интернету. Существует две основные причины этого факта: Первая — это сканирующая активность вредоносного ПО, а вторая — это обратное рассеяние, соответствующее ответному пакету, отправленному с целевого хоста, пострадавшего от DDoS-атаки.

Сканирующая атака осуществляет действия, направленные на проверку наличия уязвимости в системе безопасности узла. Фактически, они пытаются подключиться, произвольно или маршрутизируя широкий диапазон IP-адресов и номеров портов назначения, и проверяют состояние узлов назначения, просматривая их ответы. Существует два типа сканирующих атак: сканирование хоста и сканирование порта. Сканирование хоста заключается в назначении диапазона IP-адресов и попытке подключения по порядку, при этом можно узнать, назначен ли определенный хост на IP-адрес. С другой стороны, сканирование порта заключается в проверке того, находится ли порт в коммуникабельном состоянии или нет. Здесь порт — это номер сокета для идентификации прикладной программы, используемой компьютером по протоколам TCP и UDP (англ. User Datagram Protocol — протокол передачи данных, не требующий установки соединения между хостами). Например, при просмотре веб-сайта связь между двумя хостами осуществляется через порт №80.

Существует также несколько типов атак сканирования портов. SYN scan — это атака отправки SYN-пакета в TCP-коммуникации, которая известна как «Stealth Scan attach», поскольку выполняется без оставления журнала на сервере.

Для того, чтобы произвести анализ анонимной сети для поиска шаблонов трафика конкретной сканирующей атаки, используется обучение по ассоциативным правилам.

Проблема обучения ассоциативным правилам была первоначально предложена в контексте данных о рыночной корзине для поиска часто встречающихся групп товаров, которые покупаются вместе.

Обучение на ассоциативных правилах (англ. Associations rules learning — ARL) представляет из себя довольно часто применимый в реальной жизни и является методом поиска взаимосвязей (ассоциаций) в датасетах, или, если точнее, айтемсетах (англ. itemsests). В целом ARL можно определить как «Кто купил «x», также купил «y»». В основе лежит анализ транзакций, внутри каждой из которых лежит свой уникальный itemset из набора items. При помощи данных алгоритмов ведется поиск тех самых «правил» совпадения items внутри одной транзакции, которые в дальнейшем сортируются по их силе.

Предположим, существует некий датасет (или коллекция) *Dat*, такой, что *d*at = *d*at0 … *d*at*j*, где *dat* — уникальная транзакция—itemset (например, кассовый чек). Внутри каждой *dat* представлен набор *items* (*i* — *item*), причем в идеальном случае он представлен в бинарном виде:

*dat*1 = [{*Вино*: 1}, {*Вода*: 0}, {*Кола*: 1}, {...}],
*dat*2 = [{*Вино*: 0}, {*Вода*: 1}, {*Кола*: 1}, {...}].

Принято каждый itemset описывать через количество ненулевых значений (*k* — *itemset*), например, [{*Вино*: 1}, {*Вода*: 0}, {*Кола*: 1}] является 2 — *itemset*.

Если изначально датасет в бинарном виде не представлен, можно при желании его преобразовать. Таким образом, датасет представляет собой разреженную матрицу со значениями {1,0}. Это будет бинарный датасет. Существуют и другие виды записи — вертикальный датасет (показывает для каждого отдельного item вектор транзакций, где он присутствует) и транзакционный датасет (например, как в кассовом чеке).

Существует целый ряд базовых понятий в ARL:

Support (поддержка):

$$supp(X) = \frac{\{t \in T; X \in t\}}{|T|},$$

где X — itemset, содержащий в себе i—items, а T — количество транзакций. В общем виде это показатель «частотности» данного itemset во всех анализируемых транзакциях. Но это касается только X. Нам же интересен скорее вариант, когда в одном itemset встречаются x_1 и x_2 (например). Пусть $x_1 = \{Вино\}$, а $x_2 = \{Конфеты\}$, значит нам необходимо посчитать, количество транзакций, в которых встречается эта пара.

$$\text{supp}(x_1 \cup x_2) = \frac{\sigma(x_1 \cup x_2)}{|T|},$$

где σ — количество транзакций, содержащих x_1 и x_2

$$\text{supp} = \frac{\text{Транзакции с вино и конфеты}}{\text{Все транзакции}} = \\ = P(\text{Вино} \cap \text{Конфеты})$$

Confidence (достоверность):

Confidence — показатель частоты срабатывания нашего правила для всего датасета.

$$\text{conf}(x_1 \cup x_2) = \frac{\text{supp}(x_1 \cup x_2)}{\text{supp}(x_1)}.$$

Приведем пример. Допустим, что требуется рассчитать confidence для правила «кто покупает вино, тот покупает и конфеты». Сначала необходимо будет рассчитать support у правила «покупает вино», потом рассчитать его же у правила «покупает вино и конфеты», и поделить одно на другое. Другими словами, будет рассчитано в скольких случаях (транзакциях) будет работать правило «купил вино» supp(X), «купил конфеты и вино».

$$\text{conf}(\text{Вино} \cap \text{Конфеты}) = \frac{\text{supp}(\text{Вино} \cap \text{Конфеты})}{\text{supp}(\text{Вино})} = \\ = P(\text{Конфеты} \mid \text{Вино})$$

Существует несколько часто используемых алгоритмов, которые позволяют найти привила в items исходя из перечисленных выше понятий.

Рассмотрим один из них: FP-Growth/FP-tree алгоритм.

FP-Growth (Frequent Pattern Growth) более новый алгоритм, который в первые был описан в 2000 году. FP-Growth предлагает совершенно новый подход — отказаться от генерации кандидатов.

На теоретическом уровне, подобный подход позволит значительно увеличить скорость выполнения алгоритма, при этом используя гораздо меньший объем памяти. Это осуществимо за счет хранения префиксного дерева (tree) в памяти из самих транзакций, а не из комбинаций кандидатов. Также FP-Growth создает таблицу заголовков для каждого item, чей supp выше заданного пользователем.

Основная идея алгоритма FP-Growth может быть описана следующим образом:

— производится сжатие входной базы данных, создавая экземпляр FP-tree для представления часто встречающихся элементов (*frequent items*);
— после первого этапа происходит деление сжатой базы данных на набор условных данных, каждый из которых связан с одним частным шаблоном;
— на данном этапе каждый такой набор данных анализируется отдельно.

В больших базах данных удержание FP-Growth в основной памяти невозможно. Стратегия решения этой проблемы состоит в том, чтобы разделить базу данных на набор меньших баз данных (называемых спроецированными базами данных), а затем построить FP-tree из меньшего набора данных.

Древо частых наборов паттернов (FP-tree) представляет собой компактную структуру данных, в которой хранится количественная информация о частых паттернах в базе данных. Каждая транзакция считывается, а затем сопоставляется с путем в FP-tree. Это делается до тех пор, пока все транзакции не будут прочитаны. Различные транзакции с общими подмножествами позволяют дереву оставаться компактным, поскольку их пути перекрываются.

В качестве аргументов принимается набор пакетов TCP SYN и настраиваются два параметра minSup и minConf. Необходимо их определить так, чтобы количество правил было не недостаточным и не избыточным.

Если эти параметры сделать слишком малыми, то может существенно увеличится время выполнения алгоритма и найдется слишком много ненадежных правил. А если параметры будут слишком большие, то правил может вообще не найтись. Поэтому при первом запуске алгоритма рекомендуется сделать параметры поменьше, чтобы вывести как можно больше правил, а затем постепенно их уменьшать, пока количество правил не станет разумным.

minSup — это минимальная поддержка. Значение поддержки меняется от 0 (когда условие и следствие не встречаются вместе ни в одной транзакции) до 1 (когда условие и следствие во всех транзакциях появляются совместно). В общем случае поддержка является мерой надежности, с которой ассоциативное правило выражает ассоциативную связь между условием и следствием. Если поддержка $S > 0{,}8$, то связь сильная, а само правило заслуживает доверия. В случае, когда $0{,}5 < S < 0{,}8$, ассоциативная связь средняя, а правило следует использовать с осторожностью. При $S < 0{,}5$ связь слабая, а ассоциативное правило является сомнительным;

minConf — минимальная достоверность. Это показатель, характеризующий уверенность в том, что ассоциация A → B является ассоциативным правилом. То есть предположение о том, что появление события A влечёт за собой появление события B, является достаточно достоверным.

Изучение ассоциативных правил может быть выполнено в следующие два этапа:

— поиск часто встречающихся шаблонов, где каждый из наборов элементов будет удовлетворять минимальной поддержке, т.е. встречается по крайней мере так же часто, как minSup;
— генерация сильных ассоциативных правил, где правила, созданные из часто используемых наборов элементов с гарантированной минимальной поддержкой (minSup), должны удовлетворять ограничению минимальной достоверности (minConf).

Для оценки предложенного метода поиска правил использовался большой набор пакетов TCP SYN, собранных с помощью датчика Даркнета NICT/16. Всего было собрано 1.047.500 пакета, которые были отправлены с уникальных хостов. Далее выбирался порт назначения, номер последовательности и размер окна в качестве полей заголовка. Само обучение ассоциативных правил выполнялось для SYN-пакетов Даркнета. В исследовании рассматривались только те ассоциативные правила, поддержка (source hosts) и уверенность которых превышает 2.000 и 90 %.

Предполагаемый метод заключается в том, что обучение ассоциативным правилам может применятся к каждому полю заголовка для выработки полезных правил. Для этого проводилась проверка всех значений каждого поля в заголовках TCP и IP для всех собранных SYN-пакетов и определялся набор транзакций для каждого поля заголовка. Например, сосредоточившись на пяти полях заголовка: «source port», «destination port», «sequence number», «9 flags» и «window size», из собранных SYN-пакетов темной сети были получены три набора транзакций. Затем для каждого набора транзакций проводилось обучение правилам ассоциации. В Таблице 1 представлены полученные ассоциативные правила.

Таблица 1.

Таблица полученных ассоциативных правил

Association rules	Support	Confidence
(1320, 4488) → 792	10051	90.2
(1320, 2476, 4488) → 792	6657	96.0
(1320, 8456) → 792	5885	90.6
(1320, 2376, 8456) → 792	4064	95.8
(1320, 16904) → 792	3329	90.4
(1320, 4488, 8456) → 792	2886	96.3

К полученным данным в данной таблице применялся алгоритм FP-Growth из библиотеки fpgrowth_py. На ассоциативных правилах использовался эмулятор mininet, сначала была создана топология сети с 25 хостами и одновременно использован контроллер RYU (компонентная программно-определяемая сетевая среда). Создан сценарий вредоносных пакетов с помощью Python Scapy Framework с использованием подмены IP-адреса (англ. spoofing attack). Проинициализирован TCP-сервер на узле-жертвы. Произведен одновременный захват синхронных пакетов TCP с помощью Wireshark. С помощью tshark экспортирован файл формата pcap и конвертирован в файл csv.

На Рисунке 1 представлен график ассоциативных правил.

Был выявлен ряд ассоциативных правил, который продемонстрирован в Таблице 1 и на Рисунке 1.

В данной работе был проанализирован метод анализа анонимной сети с использованием обучения по ассоциативным правилам. В предложенном методе, для создания наборов транзакций для ассоциативных правил, использовались не только порты назначения, но и другая информация заголовка TCP/IP.

Обсуждение

В ходе исследования было описано, как различные устройства IoT могут стать жертвами вредоносных программ в Даркнете, в частности, программным продуктом Mirai. Для установления связей между такими программами и устройствами был исследован новый метод отслеживания с использованием ассоциативных правил, которые позволили выявить сходства в поведении Mirai. Для нахождения ассоциативных правил за основу был взят алгоритм FP-Growth, который позволяет увеличить скорость алгоритма при использовании меньшего объема памяти. Был произведен анализ пакетов TCP SYN, для которых были настроены два параметра minSup и minConf. Были выявлены этапы изучения ассоциативных правил.

Решение такой задачи должно способствовать повышению эффективности и точности обнаружения атак на устройства IoT и позволяет предотвратить дальнейшее распространение вредоносных программ в целевых сетях.

Заключение

Таким образом, анализ трафика анонимной сети с использованием ассоциативных правил может использоваться для обнаружения вредоносных программ IoT. Он позволяет идентифицировать потенциальные угрозы

Таблица 1. Полученные ассоциативные правила для размеров окон TCP.

Правила ассоциации	Поддержка	Доверие [%]
(1320, 4488) → 792	10051	90.2
(1320, 2376, 4488) → 792	6657	96.0
(1320, 8456) → 792	5885	90.6
(1320, 2376, 8456) → 792	4064	95.8
(1320, 16904) → 792	3329	90.4
(1320, 4488, 8456) → 792	2886	96.3

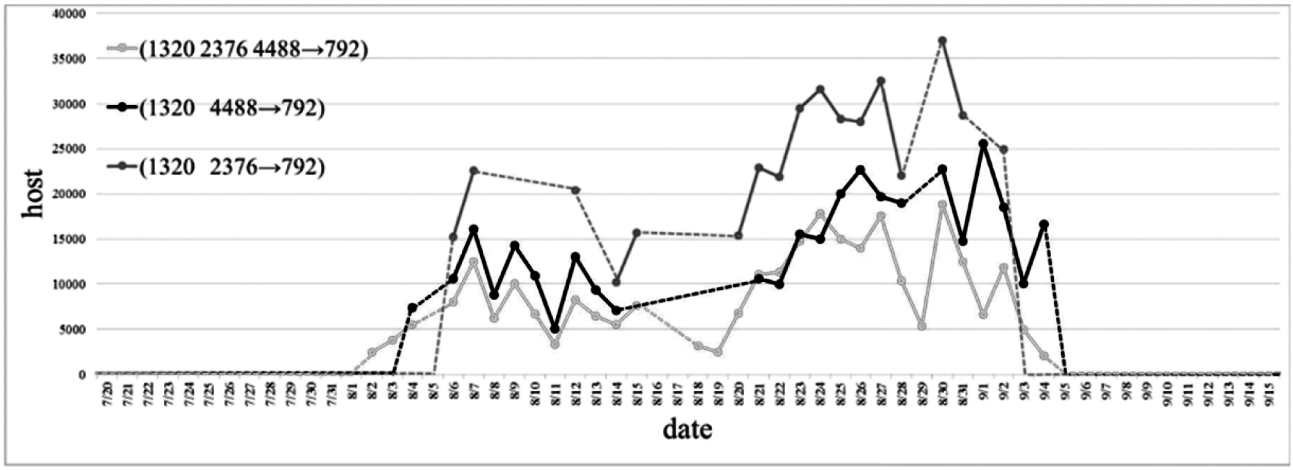

Рис. 1. Таблица полученных ассоциативных правил (Support, Confidence)

и принимать меры по их предотвращению. Кроме того, этот метод может помочь разработчикам устройств IoT усовершенствовать свой продукт, чтобы он не подвергался атакам и не становился источником угрозы для пользователей.

ЛИТЕРАТУРА

1. Павликов С.Н., Коломеец В.Ю., Колесов Ю.Ю., Петров П.Н., Афанасьев Р.К. Метод обнаружения вредоносных программ и их элементов // Наукоемкие технологии в космических исследованиях Земли. 2022. № 3. URL: https://cyberleninka.ru/article/n/metod-obnaruzheniya-vredonosnyh-programm-i-ih-elementov (дата обращения: 09.05.2023).
2. Васильев, А. Даркнет как ускользающая сфера правового регулирования / А. Васильев, Ж. Ибрагимов, О. Васильева // Юрислингвистика. — 2019. — № 12(23). — С. 10–12. — EDN CBPGEY.
3. Оралбаев ЕА. Обнаружения DDoS-атак ботнетов в сетях доступа IoT // Актуальные вопросы современной науки и образования. Монография. Пенза, 2021. С. 190–200.
4. DDoS в Интернете вещей: Mirai и другие / К. Колиас, Г. Камбуракис, А. Ставру, Д. Воас // Открытые системы. СУБД. — 2017. — № 4. — С. 12–15. — EDN ZUVUWV.
5. Кучин, Д. А. DDOS-атаки в лице ботнета Mirai / Д. А. Кучин, Т. Н. Кузнецова // Общество, государство, личность: модернизация системы взаимоотношений в современных условиях: Материалы XVIII Межвузовской научно-практической конференции студентов, магистрантов, аспирантов и молодых ученых, Казань, 27 апреля 2018 года / Под ред. А.Н. Грязнова. — Казань: Университет управления «ТИСБИ», 2018. — С. 227–229. — EDN XSFNIL.

© Куликов Александр Анатольевич (kulikov_aa@mirea.ru); Кравцова Екатерина Юрьевна (9067320378@mail.ru);
Платошин Александр Игоревич (sasaplatosin@gmail.ru).
Журнал «Современная наука: актуальные проблемы теории и практики»