УДК 004.056

АНАЛИЗ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ SSH-ХАНИПОТА COWRIE

С.Н. ПЕТРОВ[1], В.Н. РОМАНОВИЧ[2], А.А. СЕРГАНОВСКИЙ[2]

1 – Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь
2 – Национальный детский технопарк, Республика Беларусь

Поступила в редакцию 5 апреля 2024

Аннотация. Выполнено развертывание мультиханипота T-Pot на виртуальных серверах Amazon EC2 (AWS) в трех географических регионах. Выполнен анализ IP-адресов потенциальных нарушителей, взаимодействовавших с SSH-ханипотом Cowrie. Выполнен анализ логинов (имен пользователей) и паролей, использованных для подключения к ханипоту, а также команд, которые пытались выполнить нарушители. Показано, что ханипоты до сих пор могут использоваться в качестве эффективного инструмента для анализа поведения нарушителей и выявления векторов атак.

Ключевые слова: сетевые атаки, сетевая безопасность, ханипоты, Cowrie.

Введение

Сетевые атаки включают в себя различные методы, используемые нарушителями для получения несанкционированного доступа к компьютерным системам и сетям. Одной из форм сетевой атаки является сетевая разведка, процесс, при котором нарушители собирают информацию о целевой сети или системе, чтобы идентифицировать уязвимости, которые могут быть использованы для дальнейших атак. База знаний MITRE D3FEND [1] содержит описание различных вариантов противодействия техникам нарушителей. Так, один из вариантов называется Deceive, что можно перевести как обман, хитрость. Среда, которая включает в себя сервера и подключения, предназначенные для обмана нарушителя, называется Decoy Environment (обманная среда). Decoy Object (объекты-обманки) представляет собой фиктивный объект или ресурс, который создается с целью привлечения нарушителей, отвлечения их внимание от ценной информации, и обеспечить анализ и мониторинг атак. В среде специалистов по кибербезопасности такие объекты называют ханипотами (honeypot), которые представляют собой поддельные и умышленно уязвимые объекты, которые могут заинтересовать нарушителей [2]. При эксплуатации ханипотов действия нарушителя записываются и анализируются. Это позволяет получить информацию о возможных угрозах, векторах атаки и принять меры для их предотвращения. Ниже рассмотрены результаты ханипота Cowrie в составе мультиханипота T-Pot, который фиксирует попытки установления SSH- или telnet-соединений.

Практическая часть

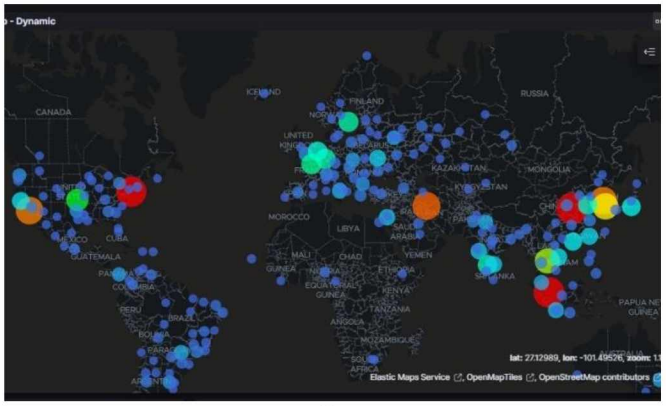
Для сбора информации T-Pot [3] был развернут в облачном сервисе AWS, позволяющем развертывать приложения и хранить данные в облаке, обеспечивая доступ к высокопроизводительным ресурсам и инфраструктуре для клиентов. Использовалась служба Amazon EC2 для аренды виртуальных выделенных серверов (instance). Всего было развернуто 3 экземпляра типа t2.large в течении 14 дней в географических регионах Северная Вирджиния, Сеул и Франкфурт.

Ханипот Cowrie показал один из наиболее высоких результатов (примерно 30000 попыток подключений во всех регионах суммарно). Ниже представлены результаты по региону Азия

(Сеул). На рис. 1 показана статистика десяти наиболее активных стран по числу попыток установить соединение, а также общая география атак.

geoip.country_name.keyword: Descending	Count
United States	4,569
South Korea	2,616
China	2,583
Singapore	1,762
Iran	1,358
India	1,279
Thailand	1,048
France	541
Sweden	509
The Netherlands	506

а



б

Рис.1 Карта атак, по данным собранным с ханипота Cowrie в Сеуле: *а* – статистика десяти наиболее активных стран по числу попыток установить соединение; *б* – общая география атак

Трафик по протоколу telnet в 2 раза превышал трафик по протоколу SSH. Десять наиболее часто используемых IP-адреса, с которых осуществлялись попытки подключений показаны на рис. 2.

Source IP	Count
110.78.138.200	1,001
218.200.189.88	956
5.234.170.153	915
142.93.76.208	778
43.156.128.13	459
120.224.174.135	420
2.183.102.137	415
51.75.127.207	400
45.95.147.174	329
54.234.73.133	308

Рис. 2 Десять наиболее активных IP-адресов

Анализируя IP-адреса при помощи сервиса VirusTotal, установили, что IP-адрес 180.214.176.3 имел отношение к вредоносному ПО Mipony, который является поддельным файловым установщиком. IP-адрес 37.139.249.103 имеет плохую репутацию и признан источником большого количества спама, расположен в России. Следующими аномалиями стали IP-адреса, с которых зафиксирована попытка использования команды «cat /bin/echo ‖ ‖while read i; do echo $i; done < /proc/self/exe» (7 адресов). Данная команда последовательно считывает содержимое файлов, указанных в параметре Файл, и записывает его в стандартный поток вывода.

При анализе остальных IP-адресов были отмечены адреса 121.186.46.238 и 210.165.104.204, первый из которых используется поддельным установщиком утилиты qBittorrent, а со второго распространяется вредоносное ПО.

Cowrie собирает и логины и пароли, используемые потенциальными нарушителями при попытках подключения по telnet или SSH. Наиболее часто используемые логины (слева) и пароли (справа) представлены на рис. 3.

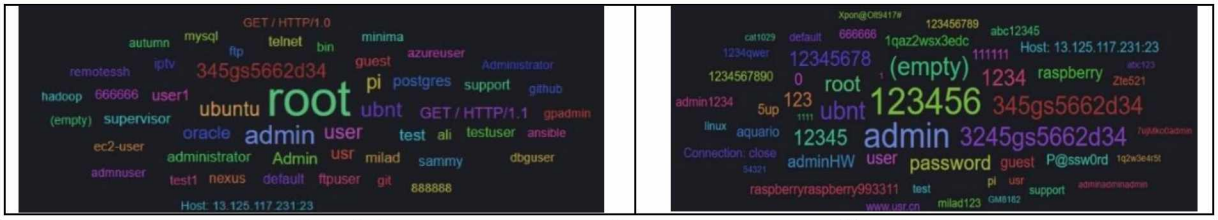


Рис. 3 Логины и пароли, собранные ханипотом Cowrie

Наиболее популярными логинами являлись: root, admin, ubnt. Среди паролей пользовались популярностью такие пароли как: admin, ubnt, 123456. В целом, среди наиболее популярных паролей зафиксированы, пароли из распространенных словарей для брутфорса. Отдельный интерес представляю пароли или логины в виде HTTP запросов, типа GET. В таких случая речь идет об SQL инъекциях (атака, которая позволяет использовать фрагмент вредоносного кода на языке SQL для манипулирования базой данных и получения доступа к потенциально ценной информации). Использование имени пользователя «pi» и паролями «raspberry» и «raspberryraspberry993311» говорит о том, что нарушитель использовал вредоносную программу Poison Dwarf (CPUminer). Были зарегистрированы попытки выполнения нарушителями команд, десятка наиболее используемых представлена на рис. 4.

Command Line Input	Count
shell	158
while read i	121
system	114
enable	78
sh	75
uname -a	63
cat /proc/cpuinfo | grep model | grep name | wc -l	54
cat /proc/cpuinfo | grep name | head -n 1 | awk '{print $4,$5,$6,$7,$8,$9;}'	54
cat /proc/cpuinfo | grep name | wc -l	54
cd ~; chattr -ia .ssh; lockr -ia .ssh	54

Рис. 4 Команды, собранные ханипотом Cowrie

Команда «shell» в различных операционных системах запускает командный интерпретатор, который позволяет пользователю вводить команды и выполнять их в рамках этой оболочки. Команда «system» в UNIX Shell выполняет внешнюю команду или программу, переданную в качестве аргумента. Она принимает один или несколько аргументов, которые затем передаются системной функции «exec» для выполнения. Эта команда обычно используется для запуска других программ или утилит из сценария UNIX Shell. Команда «kill %1» в некоторых операционных системах используется для закрытия процесса с идентификатором, записанным в виде символа процента (%1) в командной строке.

Результаты для региона Северная Вирджиния и Франкфурт во многом схожи. Для региона Северная Вирджиния Cowrie зафиксировал 12794 атаки, которые использовали telnet и SSH уязвимости в равном соотношении. Большинство атак исходило из США, Индонезии и Китая. Был произведен анализ списка 10 самых частых IP-адресов нарушителей (рис. 5).

Проанализировав три самых популярных IP адреса в этом списке, поскольку количество их атак значительно превышает количество атак с остальных IP. 103.144.38.42, 97.74.91.196, 124.230.124.250. По данным VirusTotal все три адреса имеют плохую репутацию и признаны источниками большого количества спама.

Наиболее используемыми логинами стали: root 787 раз, admin 171 раз, test 86 раз. А наиболее используемыми паролями стали:123456 - 168, root - 58, admin - 57.

Для локации Франкфурт самыми популярными логами являются: root - 300, admin - 256, user - 31. Самыми популярными паролями являются: 123456 - 34, password - 33, admin - 28. Самой

популярной связкой логина и пароля является: root/admin - 19. В ходе анализа популярных команд, введенных нарушителям самыми часто используемыми, являются: shell - 156, system - 154, enable - 78.

Source IP	Count
103.144.38.42	3140
97.74.91.196	654
124.230.124.250	619
170.64.169.161	411
5.237.234.238	392
36.139.63.59	285
149.56.117.144	213
185.200.244.137	210
201.20.56.106	163
24.223.97.5	150

Рис. 5 Список 10 наиболее популярных IP-адресов (Северная Вирджиния)

Заключение

Выполнено развертывание T-Pot на виртуальных серверах Amazon EC2 (AWS) в трех географических регионах. В каждом регионе T-Pot фиксировал сотни тысяч различных событий, фактов взаимодействия с ханипотами. Выполнен анализ IP-адресов потенциальных нарушителей, взаимодействовавших с Cowrie. Выполнен анализ логинов (имен пользователей) и паролей, использованных для подключения к ханипоту, а также команд, которые пытались выполнить нарушители. Наиболее распространенные связки логин плюс пароль берутся из словарей для брутфорса. Часто, они входят в «топ 10 худших паролей». Другой популярный вариант – ввод использование SQL-запросов в поле логина и пароля, для выполнения на сервере произвольных команд (SQL-инъекция). Показано, что ханипоты до сих пор могут использоваться в качестве эффективного инструмента для анализа поведения нарушителей и выявления векторов атак. Однако в силу того, что потенциальные нарушители могут обнаруживать и идентифицировать ханипоты, более перспективным решением являются решения класса Distributed Deception Platform.

ANALYSIS OF INFORMATION SECURITY EVENTS USING COWRIE SSH HONEYPOT

S.N PETROV, V.N. ROMANOVICH, A.A. SERGANOVSKY

Abstract. The T-Pot has been deployed on Amazon EC2 (AWS) virtual servers in three geographical regions. The analysis of the IP addresses of potential intruders who interacted with the Cowrie SSH honeypot was performed. The analysis of logins (usernames) and passwords used to connect to the honeypot, as well as commands that the violators tried to execute, was performed. It is shown that honeypots can still be used as an effective tool for analyzing the behavior of violators and identifying attack vectors.

Keywords: network attacks, network security, honeypots, Cowrie.

Список литературы

1. D3FEND Matrix | MITRE D3FEND [Электронный ресурс] – Режим доступа: https://d3fend.mitre.org Дата доступа: 05.04.2024
2. Путято М. М., Макарян А. С., Чич Ш. М., Маркова В. К. Исследование применения технологии Deception для предотвращения угроз кибербезопасности // Прикаспийский журнал: управление и высокие технологии. – 2020. – №4 (52). – С. 85-98
3. T-Pot – The All In One Multi Honeypot Platform [Электронный ресурс] – Режим доступа: https://github.com/telekom-security/tpotce?ysclid=lrzaidhujg725907509 Дата доступа: 05.04.2024