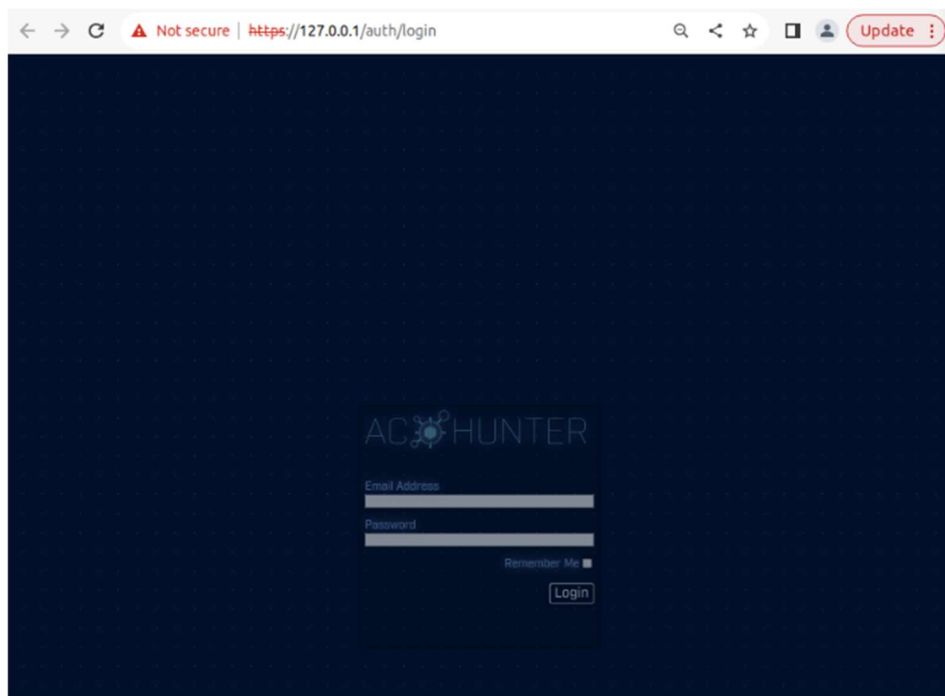


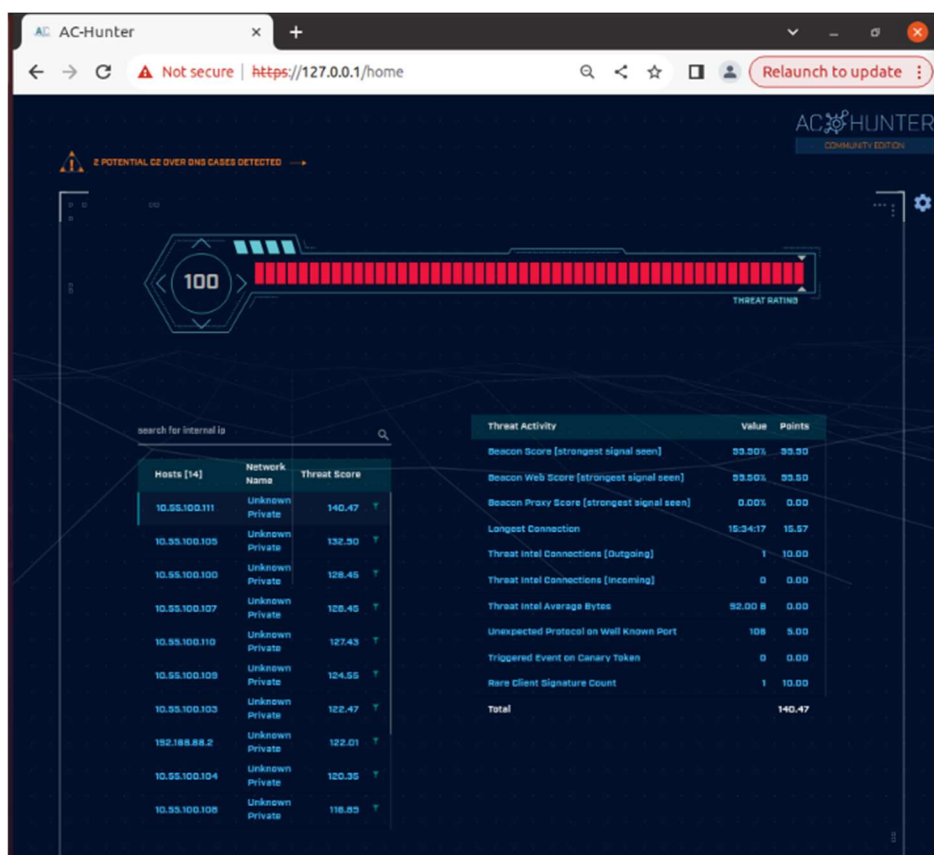
Практическая работа №4 Network Threat Hunting

Выполнил студент - Князева Анастасия Михайловна группы: ББМО-01-23

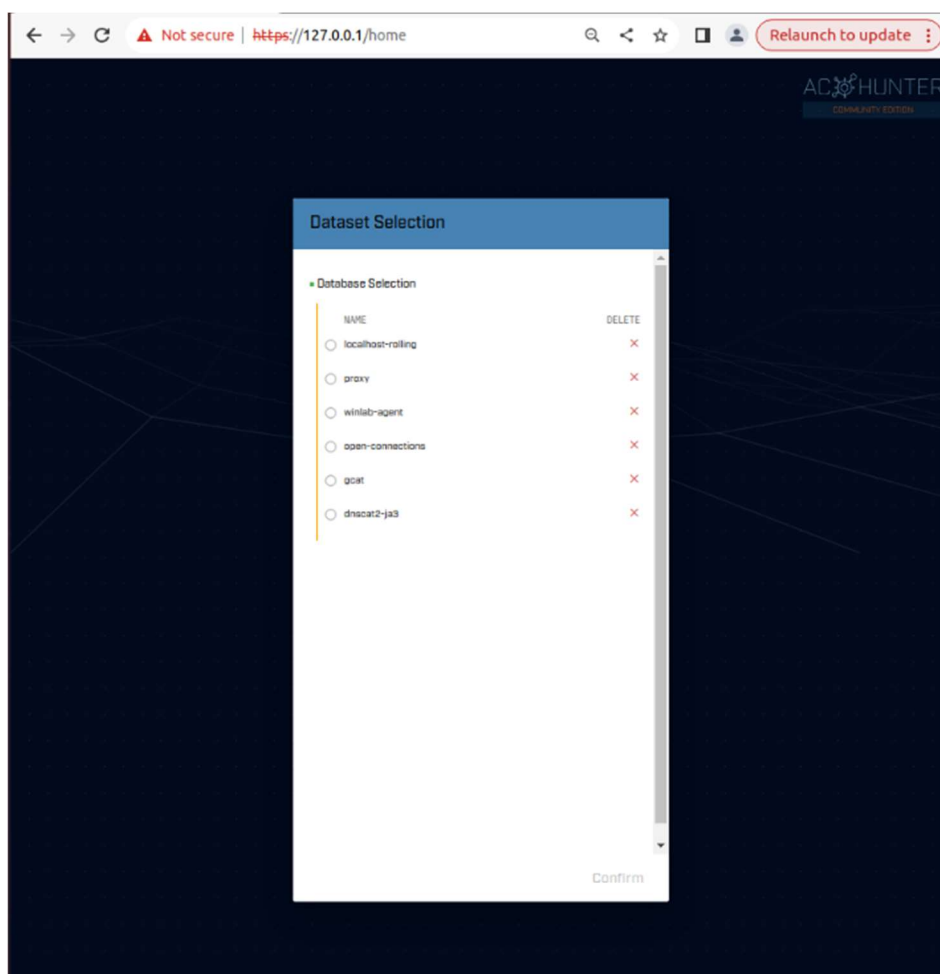
Скачиваем и разворачиваем стенд

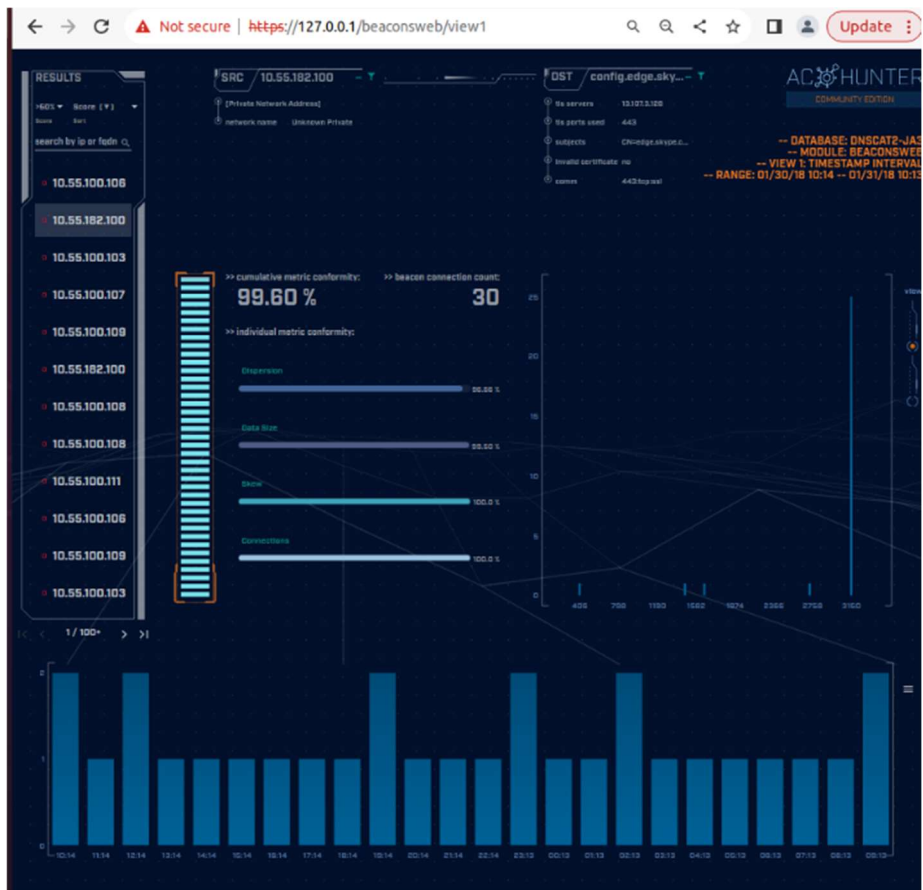


Логинимся



Добавляем адрес с трафиком к skype.com в safelist, как сказано в руководстве





← → ↻ 🔒 Not secure | https://127.0.0.1/beaconsweb/view1 🔍 ⌂ ⓘ Update

RESULTS
+601 Score (▼)
Name Sort
search by ip or fqdn 🔍
10.55.100.106
10.55.182.100
10.55.100.103
10.55.100.107
10.55.100.109
10.55.182.100
10.55.100.108
10.55.100.108
10.55.100.108
10.55.100.111
10.55.100.106
10.55.100.109
10.55.100.103

SRC 10.55.182.100
[Private Network Address]
network name: Unknown Private

DST config.edge.sky...
to servers 131213.108
to ports used 443
subjects C:\config.edge.sky...
install certificate no
exams 443 top red

AC Hunter
COMMUNITY EDITION
-- DATABASE: DNSCAT2-JA3
-- MODULE: BEACONSWEB
-- VIEW: TIMESTAMP INTERVAL
-- RANGE: 01/30/18 10:14 -- 01/31/18 10:13

Safelist this Entry?

SRC DOMAIN

Safelist by Domain

View/edit your full safelist in Home > Settings > Safelist.

Safelist From ...

- ☒ Safelist FQDN for all internal hosts
- ☐ 10.55.182.100
- ☐ 10.55.182.0/24

Select A Resolved FQDN ...

config.edge.skype.com

Match Type ...

- ☒ enable wildcard

Safelist Pattern ...

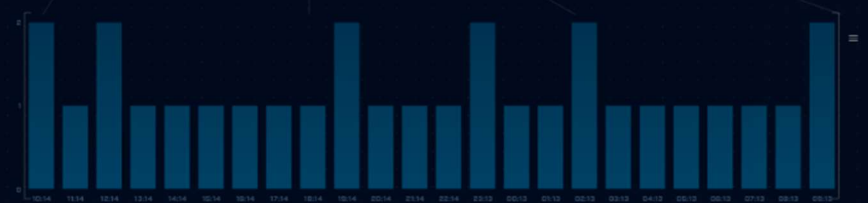
config*.edge.skype.com

Comment

Skype traffic

Cancel Safelist

1 / 100+ > >



2 POTENTIAL C2 OVER DNS CASES DETECTED

VIEW / EDIT GLOBAL SAFELIST

Global Safelist Entries

Search
Ex. 10.10.10.10

type --- scope ---

name ↑	type	scope	comment	actions
*.edge.skype.com	domain_pattern		Skype traffic	▼ ✕

1/1

Close

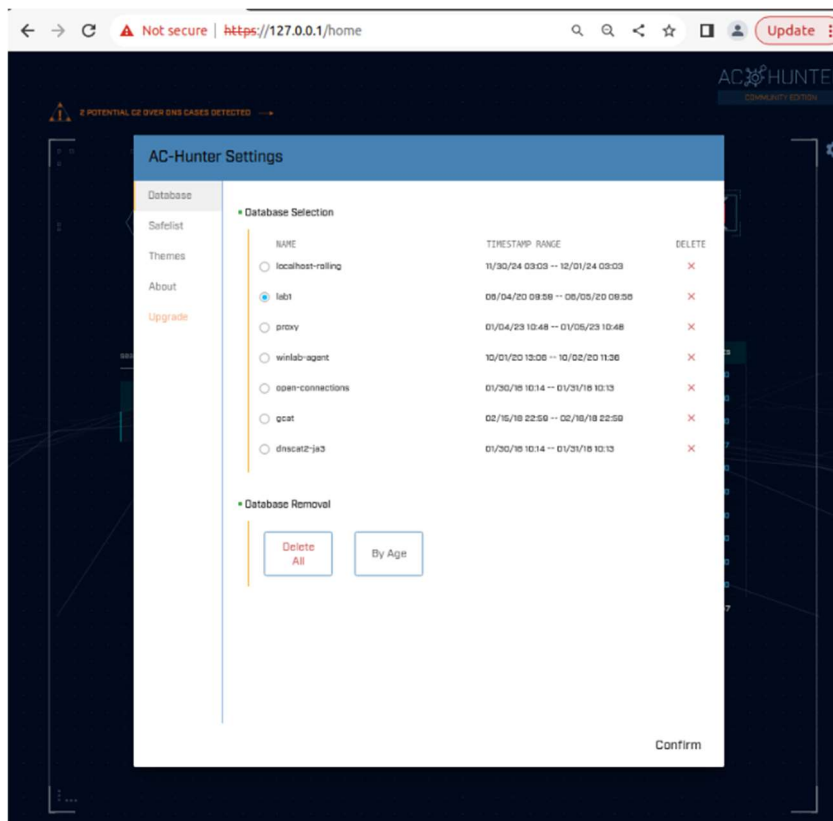
Lab 1

Импортируем логи и переключаемся на них в стенде

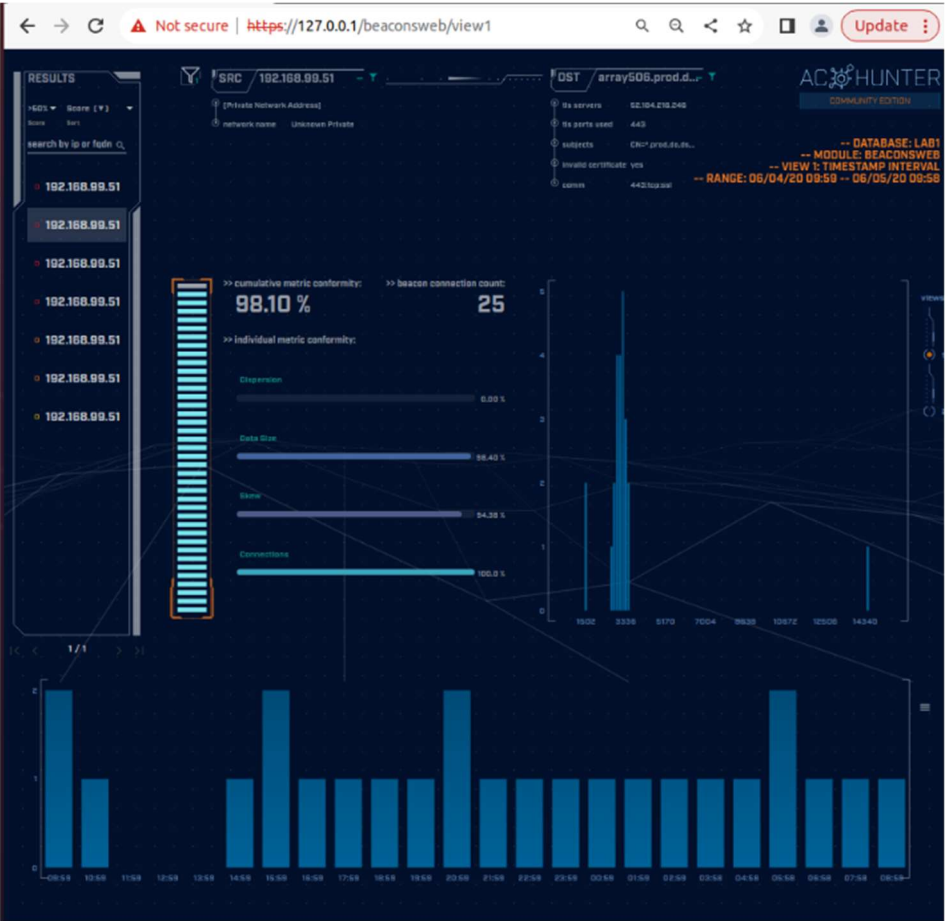
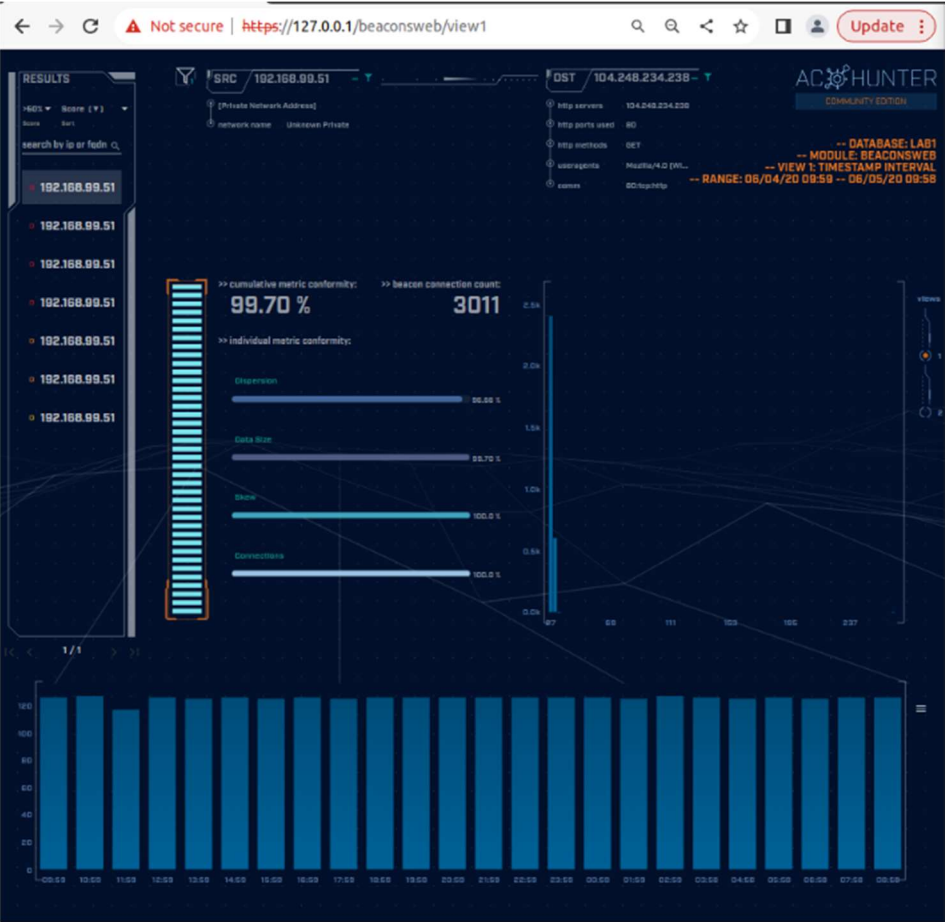
```
threat@ubuntu:~$ cd labs/lab
lab1/ lab2/ lab3/
threat@ubuntu:~$ cd labs/lab
lab1/ lab2/ lab3/
threat@ubuntu:~$ cd labs/lab1
threat@ubuntu:~/labs/lab1$ rita import *.log lab1
[sudo] password for threat:
Creating achunter_api_run ... done

[+] Importing [/home/threat/labs/lab1/capture_loss.log /home/threat/labs/lab1/conn.log /
home/threat/labs/lab1/dhcp.log /home/threat/labs/lab1/dns.log /home/threat/labs/lab1/files.log /
home/threat/labs/lab1/http.log /home/threat/labs/lab1/known_hosts.log /home/threat/labs/lab1/kno
wn_services.log /home/threat/labs/lab1/loaded_scripts.log /home/threat/labs/lab1/notice.log /hom
e/threat/labs/lab1/ntp.log /home/threat/labs/lab1/packet_filter.log /home/threat/labs/lab1/softw
are.log /home/threat/labs/lab1/ssl.log /home/threat/labs/lab1/stats.log /home/threat/labs/lab1/x
509.log]:
[-] Verifying log files have not been previously parsed into the target dataset ...
[-] Processing batch 1 of 1
[-] Parsing logs to: lab1 ...
[-] Parsing /home/threat/labs/lab1/conn.log -> lab1
[-] Parsing /home/threat/labs/lab1/dns.log -> lab1
[-] Parsing /home/threat/labs/lab1/http.log -> lab1
[-] Parsing /home/threat/labs/lab1/ssl.log -> lab1
[-] Finished parsing logs in 204ms
[-] Host Analysis: 111 / 111 [=====] 100 %
[-] Unique Connection Analysis: 110 / 110 [=====] 100 %
[-] Unique Connection Aggregation: 1 / 1 [=====] 100 %
[!] No Proxy Uconn data to analyze
[-] SNI Connection Analysis: 40 / 40 [=====] 100 %
[-] Exploded DNS Analysis: 116 / 116 [=====] 100 %
[-] Hostname Analysis: 116 / 116 [=====] 100 %
[-] Beacon Analysis: 110 / 110 [=====] 100 %
[-] Beacon Aggregation: 1 / 1 [=====] 100 %
[!] No Proxy Beacon data to analyze
[-] SNI Beacon Analysis: 40 / 40 [=====] 100 %
[-] SNI Beacon Aggregation: 1 / 1 [=====] 100 %
[-] UserAgent Analysis: 8 / 8 [=====] 100 %
[-] UserAgent Aggregation: 8 / 8 [=====] 100 %
[-] Invalid Cert Analysis: 24 / 24 [=====] 100 %
[-] Indexing log entries ...
[-] Updating metadatabase ...
[-] Done!
```

Выбираем нужный Database



Переходим в модуль beacon web и анализируем



Анализ всех адресов показал, что:

- Высокий уровень согласованности метрик (99.70%):

Такая высокая согласованность (cumulative metric conformity) может свидетельствовать о регулярных, четко упорядоченных запросах от источника к целевому IP-адресу. Это может быть признаком Beaconing-a, когда зараженное устройство связывается с управляющим сервером (C2).

- Общее количество соединений (3011):

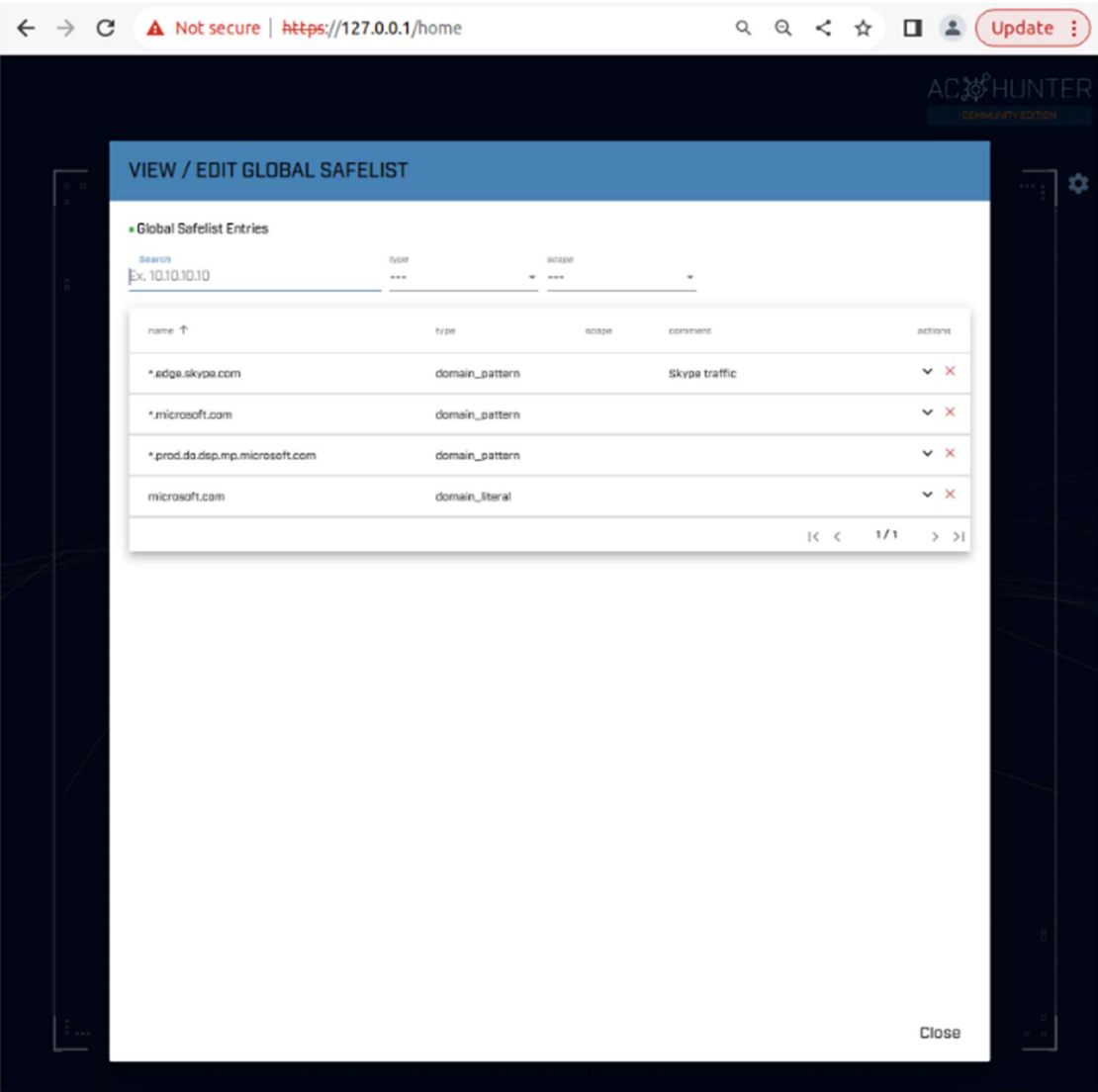
Для одного IP-адреса это значительное количество соединений. Если это типично для сети, возможно, это не аномалия. Но если такая активность не ожидается (например, для обычного пользователя или устройства IoT), это может указывать на нежелательное поведение. Равномерное распределение активности на графике:

- Использование HTTP без шифрования:

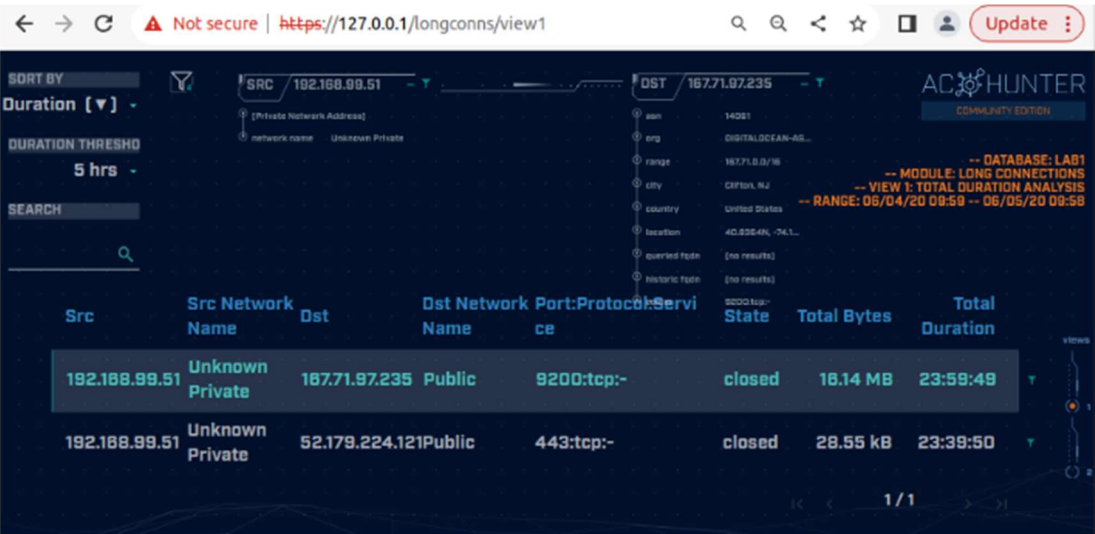
Отсутствие HTTPS может означать, что данные передаются в незашифрованном виде, что рискованно. Для связи с C2-серверами часто используются такие незащищенные протоколы.

Практически все адреса связаны с Windows, так что добавляем их в safelist

Конечный safelist



Перейдём в модуль длительных соединений



Всего 2 адреса, проверим их через VirusTotal

The screenshot shows the VirusTotal report for IP address 187.71.57.235. The interface is dark-themed. At the top, a green circle with the number '1' indicates that 1 out of 14 security vendors flagged this IP as malicious. Below this, the IP address and its AS (AS 14961 - DIGITALOCEAN-ASN) are displayed. The 'DETECTION' tab is selected, showing a table of detections. The table has columns for Date resolved, Detections, Resolver, and Domain. The data shows two detections from VirusTotal on 2023-11-14 and 2023-09-23, both for the domain piensordcad6302755c.aiihosted.com. The 'FILES REFERRING' section shows one file, file2023_export_bookmark.html, scanned on 2023-10-23. The 'HISTORICAL WHOIS LOOKUPS' section shows four lookups from 2024-06-26 to 2024-06-03, all for DigitalOcean, LLC.

Date resolved	Detections	Resolver	Domain
2023-11-14	0 / 14	VirusTotal	piensordcad6302755c.aiihosted.com
2023-09-23	0 / 14	VirusTotal	demo1.aiihosted.com

Scanned	Detections	Type	Name
2023-10-23	0 / 57	unknown	file2023_export_bookmark.html

Last Updated	Organization	Email	
2024-06-26	DigitalOcean, LLC	abuse@digitalocean.com	
2023-10-21			
2023-08-23			
2024-06-03	DigitalOcean, LLC	abuse@digitalocean.com	

The screenshot shows the VirusTotal report for IP address 32.179.224.121. The interface is dark-themed. At the top, a green circle with the number '0' indicates that 0 out of 14 security vendors flagged this IP as malicious. Below this, the IP address and its AS (AS 8075 - MICROSOFT-CORP-MSN-AS-BLOCK) are displayed. The 'DETECTION' tab is selected, showing a table of detections. The table has columns for Date resolved, Detections, Resolver, and Domain. The data shows multiple detections from various resolvers including VirusTotal, Georgia Institute of Technology, Offensive Security, and Microsoft, all for domains related to windows.notifytrafficmanager.net. The 'FILES REFERRING' section shows one file, file2023_export_bookmark.html, scanned on 2023-10-23. The 'HISTORICAL WHOIS LOOKUPS' section shows four lookups from 2024-06-26 to 2024-06-03, all for DigitalOcean, LLC.

Date resolved	Detections	Resolver	Domain
2023-06-28	0 / 14	VirusTotal	miexshdp1hlywmdc7cloudapp.azure.com
2022-09-11	0 / 14	VirusTotal	asap-cstuc2-testpage.azure.com
2022-01-10	0 / 14	VirusTotal	miexshdp1hlywmdc7cloudapp.azure.com
2021-02-06	0 / 14	Georgia Institute of Technology	amirc121msl.notifytrafficmanager.net
2021-02-03	0 / 14	Offensive Security	ckyl-fw.wms.windows.com
2021-01-31	0 / 14	Georgia Institute of Technology	wms.notifytrafficmanager.net
2021-01-24	0 / 14	Georgia Institute of Technology	brdquams.notifytrafficmanager.net
2021-01-22	0 / 14	VirusTotal	vld2-0nlp.wms.notifytrafficmanager.net
2020-10-29	0 / 14	VirusTotal	client.wms.windows.com
2019-12-12	0 / 14	VirusTotal	brdquams.notify.windows.com.akadns.net

VirusTotal пометил один из адресов, как вредоносный.

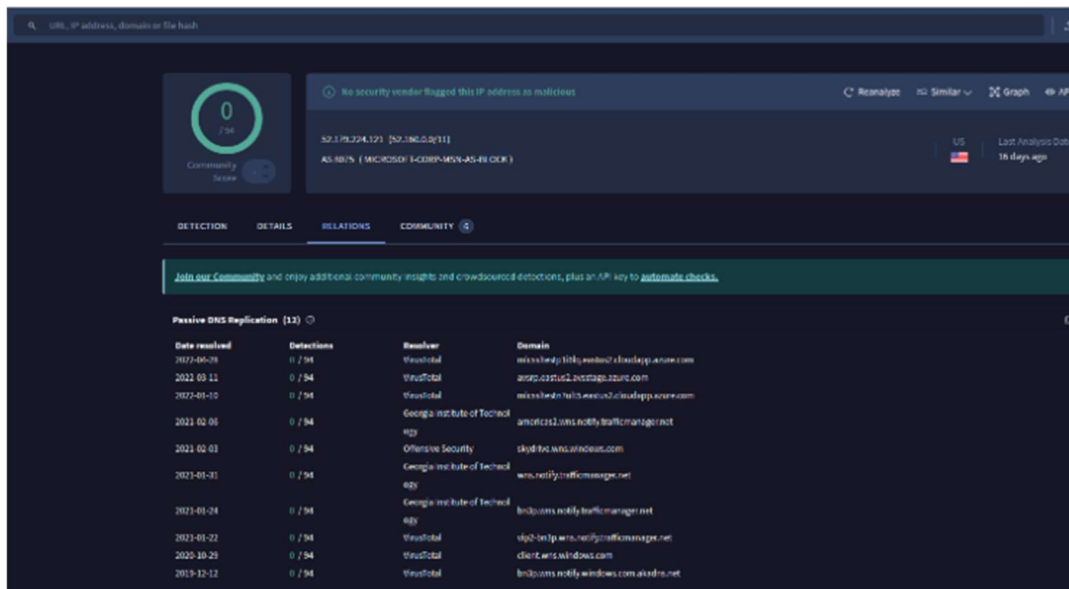
Подозрительная природа доменов Связанные с IP домены piensordcad6302755c.aiihosted.com и demo1.aiihosted.com выглядят подозрительно: Длинные, автоматически сгенерированные имена часто используются злоумышленниками для маскировки. Домены связаны с поддоменами aiihosted.com, что может указывать на временную инфраструктуру (например, для фишинга, C2 или ботнетов).

Связь с DigitalOcean Этот IP принадлежит хостинг-провайдеру DigitalOcean, который, как и другие публичные облачные провайдеры, часто используется для легальных целей. Однако злоумышленники также арендуют облачные серверы для вредоносной активности, таких как: Развёртывание C2-серверов. Проведение атак (например, DDoS, фишинг).

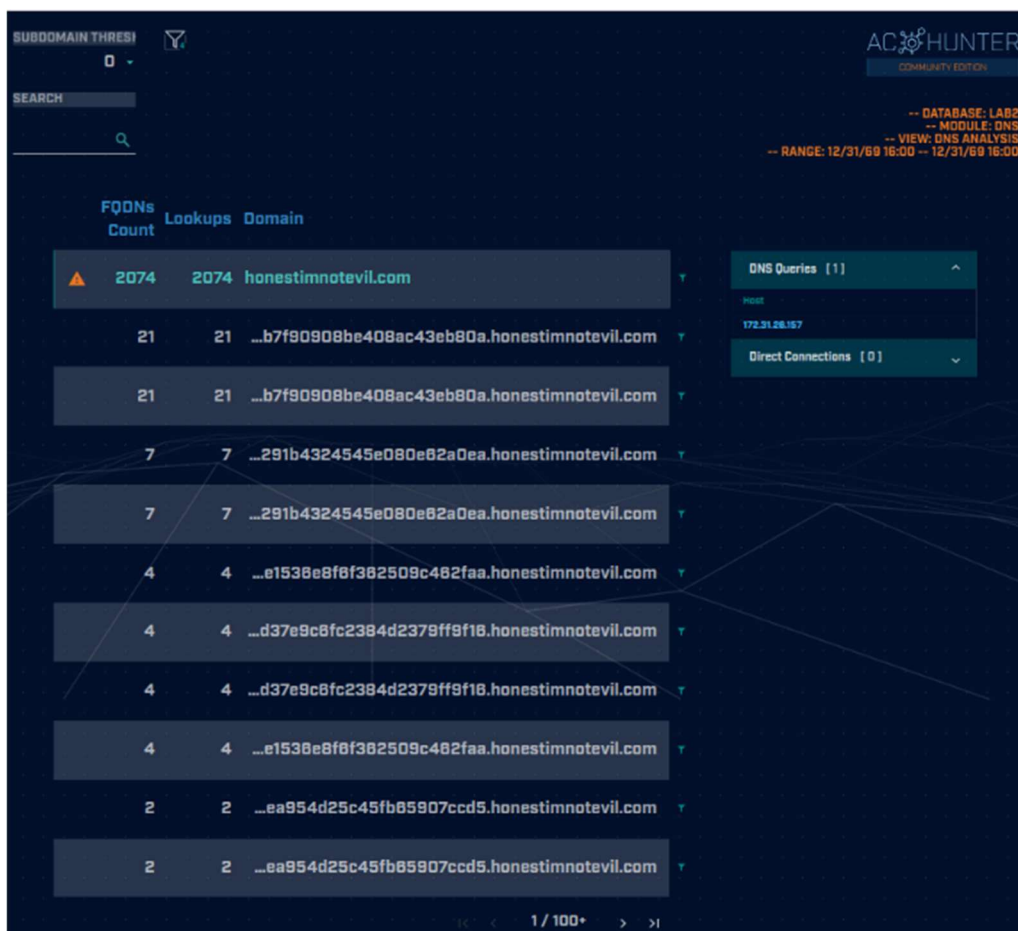
Связь с файлом "7May2021_export_bookmark.html": Хотя файл не был помечен как вредоносный, сама его природа (экспорт закладок) может намекать на использование IP для передачи данных, что требует дополнительного анализа.

Lab 2

Импортируем логи и переключаемся на них.



На основной странице пусто, но система отсылается к модулю DNS, убираем фильтры



Подозрительный домен: honestimnotevil.com Название домена вызывает подозрения из-за своей провокационной природы ("честно, я не злой"), что

может быть попыткой злоумышленников замаскировать свои намерения. Такие имена доменов часто используют в тестовых или вредоносных инфраструктурах.

Большое количество запросов (2074 запросов) Это аномальное количество DNS-запросов к одному домену, что может свидетельствовать о: Подключении к Command & Control серверу. Вредоносной программе, регулярно обращающейся к этому домену.

Длинные поддомены

Например: ...b7f9090b8e40bac43eb80a.honestimnotevil.com
...291b4324545e080e82a0ea.honestimnotevil.com

Длинные, случайно сгенерированные поддомены часто используются в доменной генерации (DGA — Domain Generation Algorithm), которая характерна для вредоносных программ. Каждый новый поддомен может быть связан с уникальной сессией или устройством, участвующим в ботнете.

Связь с единственным хостом: 172.21.8.157 Все запросы направлены на один IP-адрес (172.21.8.157). Это может быть внутренний сервер или прокси для перенаправления запросов, но такой концентрации трафика стоит уделить внимание.

Нет прямых соединений (Direct Connections = 0) Указано, что прямые соединения отсутствуют, что говорит о том, что злоумышленники могут использовать DNS-туннелирование для передачи данных через DNS-запросы. Что меня смущает: DNS-туннелирование или C2-активность

Количество запросов и странные поддомены сильно указывают на DNS-туннелирование или связь с Command & Control сервером. DGA (Domain Generation Algorithm)

Автоматически сгенерированные поддомены и подозрительный основной домен усиливают вероятность того, что это вредоносная инфраструктура. Аномальная активность в сети

Если это единственный хост (172.21.8.157), отправляющий такие запросы, он может быть скомпрометированным устройством.

Lab 3

```
threat@ubuntu:~$ cd labs/lab3
threat@ubuntu:~/labs/lab3$ rita import *.log lab3
Creating achunter_api_run ... done

[+] Importing [/home/threat/labs/lab3/capture_loss.log /home/threat/labs/lab3/conn.log /
/home/threat/labs/lab3/dhcp.log /home/threat/labs/lab3/dns.log /home/threat/labs/lab3/files.log /
/home/threat/labs/lab3/http.log /home/threat/labs/lab3/known_hosts.log /home/threat/labs/lab3/kno
wn_services.log /home/threat/labs/lab3/loaded_scripts.log /home/threat/labs/lab3/notice.log /hom
e/threat/labs/lab3/ntp.log /home/threat/labs/lab3/packet_filter.log /home/threat/labs/lab3/softw
are.log /home/threat/labs/lab3/ssl.log /home/threat/labs/lab3/stats.log /home/threat/labs/lab3/x
509.log]:
[-] Verifying log files have not been previously parsed into the target dataset ...
[-] Processing batch 1 of 1
[-] Parsing logs to: lab3 ...
[-] Parsing /home/threat/labs/lab3/ssl.log -> lab3
[-] Parsing /home/threat/labs/lab3/conn.log -> lab3
[-] Parsing /home/threat/labs/lab3/dns.log -> lab3
[-] Parsing /home/threat/labs/lab3/http.log -> lab3
[-] Finished parsing logs in 198ms
[-] Host Analysis: 88 / 88 [=====] 100 %
[-] Unique Connection Analysis: 87 / 87 [=====] 100 %
[-] Unique Connection Aggregation: 1 / 1 [=====] 100 %
[!] No Proxy Uconn data to analyze
[-] SNI Connection Analysis: 31 / 31 [=====] 100 %
[-] Exploded DNS Analysis: 107 / 107 [=====] 100 %
[-] Hostname Analysis: 107 / 107 [=====] 100 %
[-] Beacon Analysis: 87 / 87 [=====] 100 %
[-] Beacon Aggregation: 1 / 1 [=====] 100 %
[!] No Proxy Beacon data to analyze
[-] SNI Beacon Analysis: 31 / 31 [=====] 100 %
[-] SNI Beacon Aggregation: 1 / 1 [=====] 100 %
[-] UserAgent Analysis: 8 / 8 [=====] 100 %
[-] UserAgent Aggregation: 8 / 8 [=====] 100 %
[-] Invalid Cert Analysis: 18 / 18 [=====] 100 %
[-] Indexing log entries ...
[-] Updating metadatabase ...
[-] Done!
```

← → ↻ ⚠ Not secure | <https://127.0.0.1/home> 🔍 🔍 ⏪ ⭐ 🏠 👤 Update ⋮

AC-HUNTER
COMMUNITY EDITION

AC-Hunter Settings

Database

Safelist

Themes

About

Upgrade

Database Selection

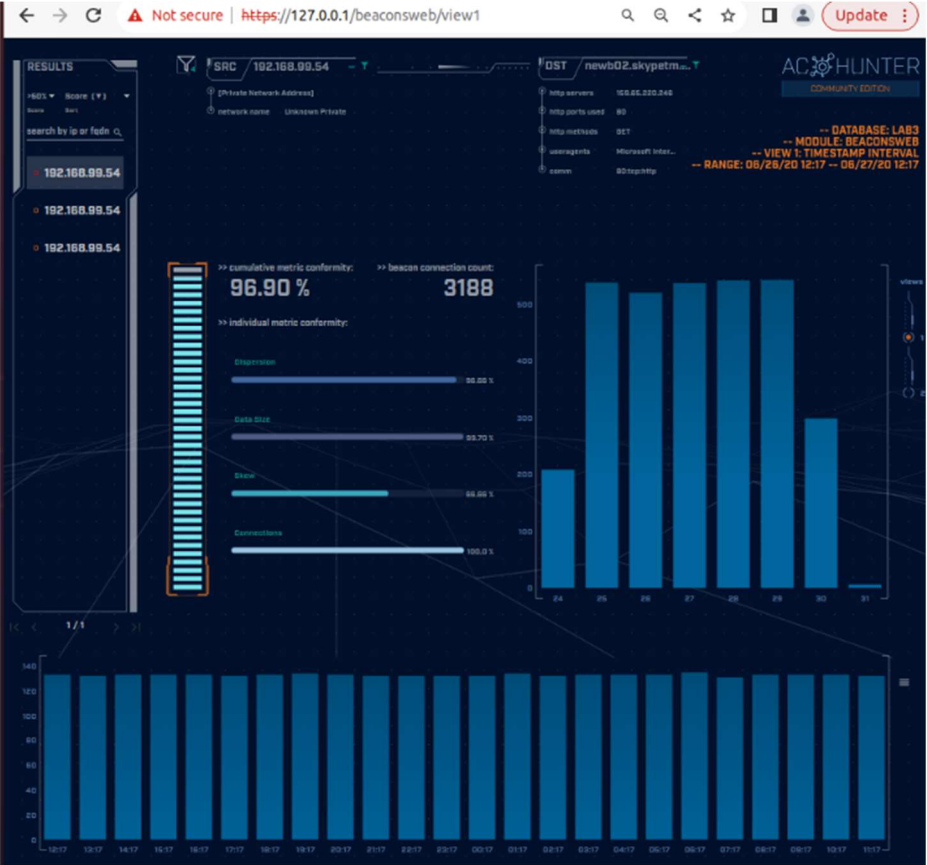
NAME	TIMESTAMP RANGE	DELETE
<input type="radio"/> localhost-rolling	11/30/24 03:03 -- 12/01/24 03:03	✗
<input checked="" type="radio"/> lab3	06/26/20 12:17 -- 06/27/20 12:17	✗
<input type="radio"/> lab2	12/31/89 16:00 -- 12/31/89 16:00	✗
<input type="radio"/> lab1	06/04/20 09:56 -- 06/05/20 06:56	✗
<input type="radio"/> proxy	01/04/23 10:48 -- 01/05/23 10:48	✗
<input type="radio"/> winlab-agent	10/01/20 13:06 -- 10/02/20 11:56	✗
<input type="radio"/> open-connections	01/30/18 10:14 -- 01/31/18 10:13	✗
<input type="radio"/> qcat	02/15/18 22:50 -- 02/16/18 22:50	✗
<input type="radio"/> dnscat2-jab3	01/30/18 10:14 -- 01/31/18 10:13	✗

Database Removal

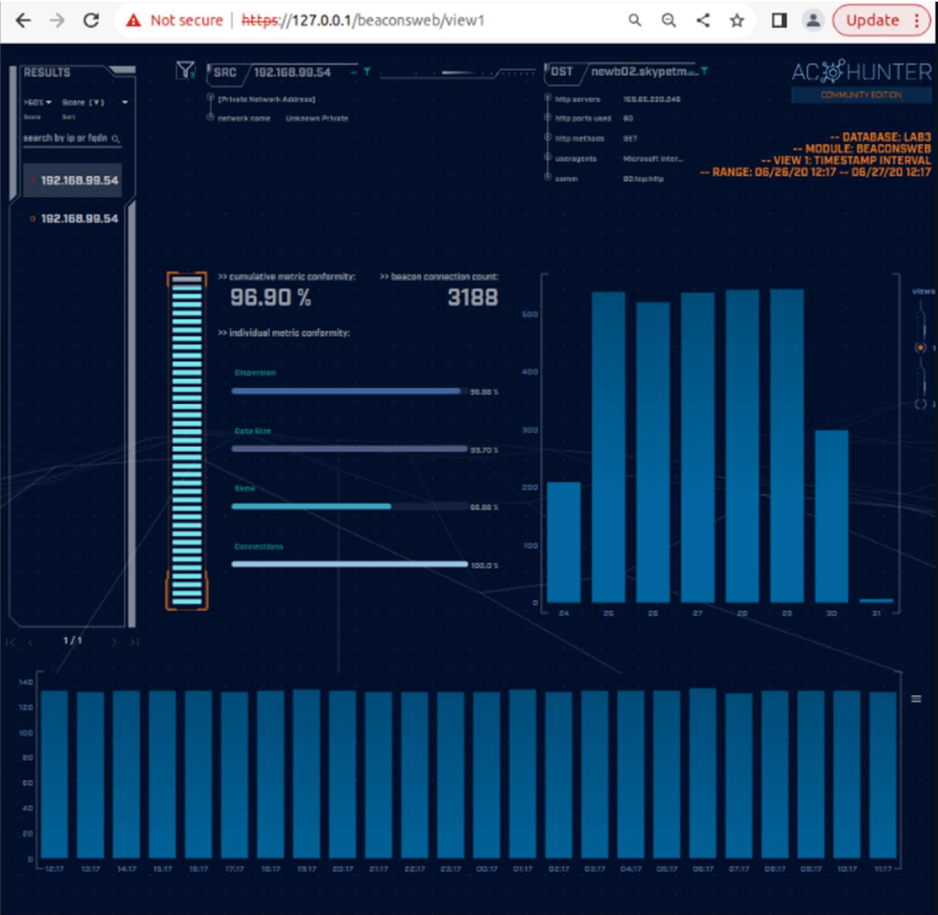
Delete All By Age

Confirm

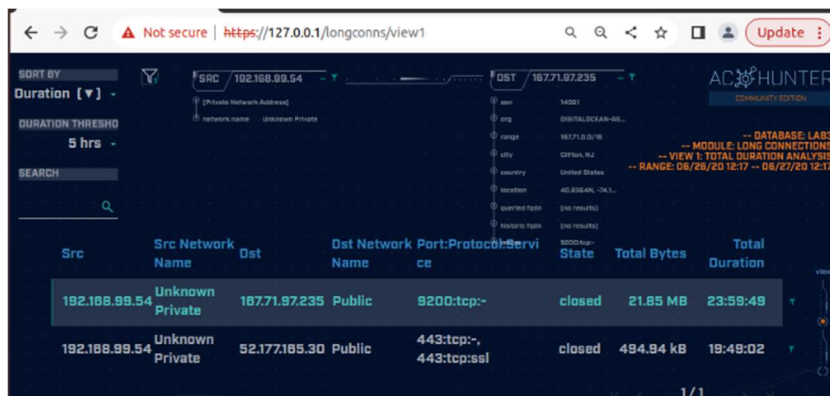
Переходим в модуль beacons web



Анализируем адреса и вносим легитивные в safelist



Остается всего два адреса, проверим каждый через VirusTotal



The screenshot shows the ACX Hunter web interface. At the top, there's a search bar with 'SRC' set to '192.168.99.54' and 'DST' set to '167.71.97.235'. Below this, there's a table with columns: Src, Src Network Name, Dst, Dst Network Name, Port:Protocol:Service, Status, Total Bytes, and Total Duration. Two rows of data are visible. The first row shows a connection to 167.71.97.235 on port 9200 (tcp) with a status of 'closed', 21.85 MB of data, and a duration of 23:59:49. The second row shows a connection to 52.177.185.30 on port 443 (tcp) with a status of 'closed', 494.94 kB of data, and a duration of 19:49:02. On the right side, there's a sidebar with various filters and a 'Update' button.

Src	Src Network Name	Dst	Dst Network Name	Port:Protocol:Service	Status	Total Bytes	Total Duration
192.168.99.54	Unknown Private	167.71.97.235	Public	9200:tcp:-	closed	21.85 MB	23:59:49
192.168.99.54	Unknown Private	52.177.185.30	Public	443:tcp:-, 443:tcp:ssl	closed	494.94 kB	19:49:02

Связь с вредоносной активностью

Метка DGA и упоминание Cobalt Strike усиливают подозрения, что домен используется для управления вредоносной активностью. Количество детекций

Пять независимых сервисов отметили домен как вредоносный, что повышает вероятность его использования в атаках. Неопределённость IP-адреса

IP 210.71.232.11 необходимо анализировать отдельно. Если он используется несколькими подозрительными доменами, это усилит подозрения. Свежесть данных

Анализ проводился месяц назад, что недостаточно актуально для оценки текущей активности домена.