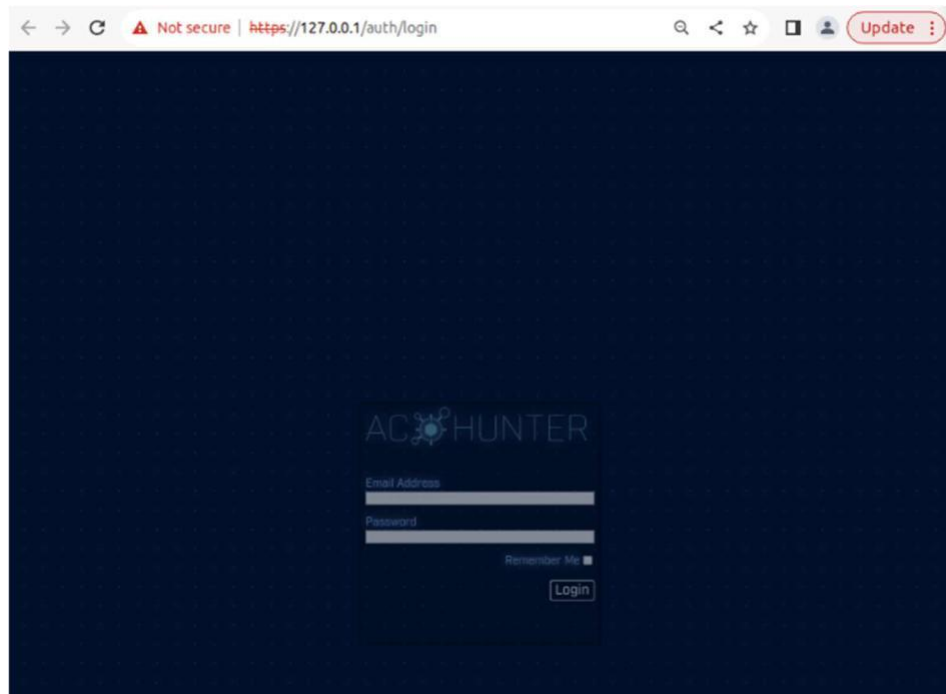


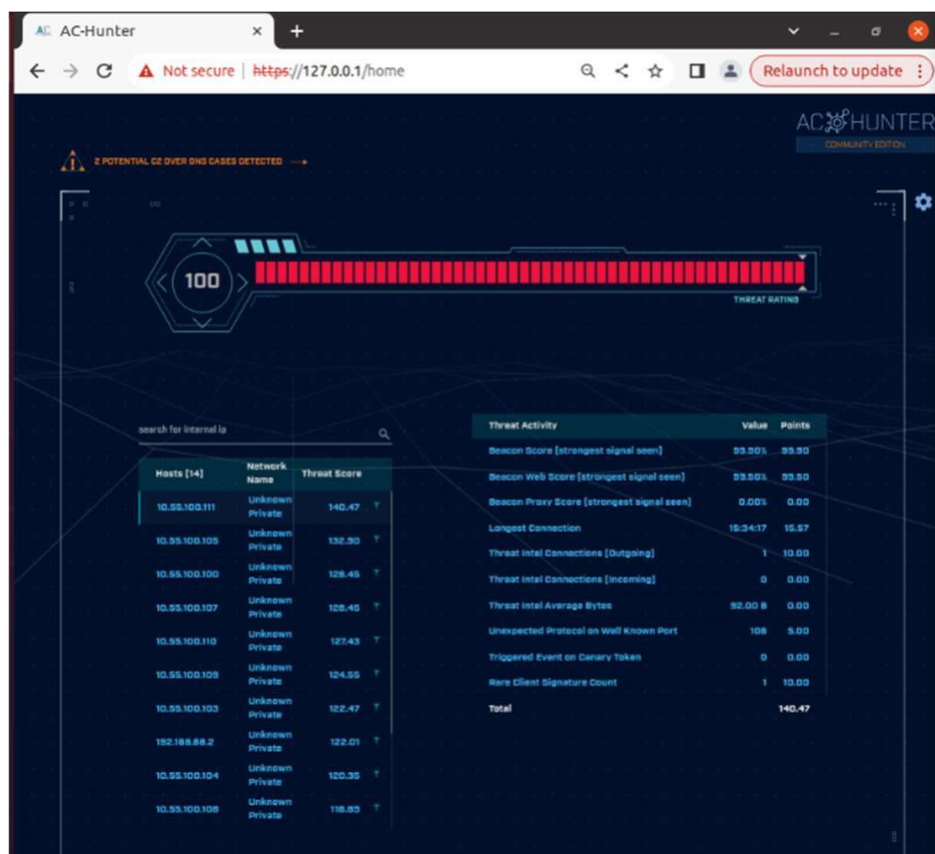
Практическая работа №4 Network Threat Hunting

Практическую работу выполнил Сапов Александр Дмитриевич, студент группы БМО-02-23

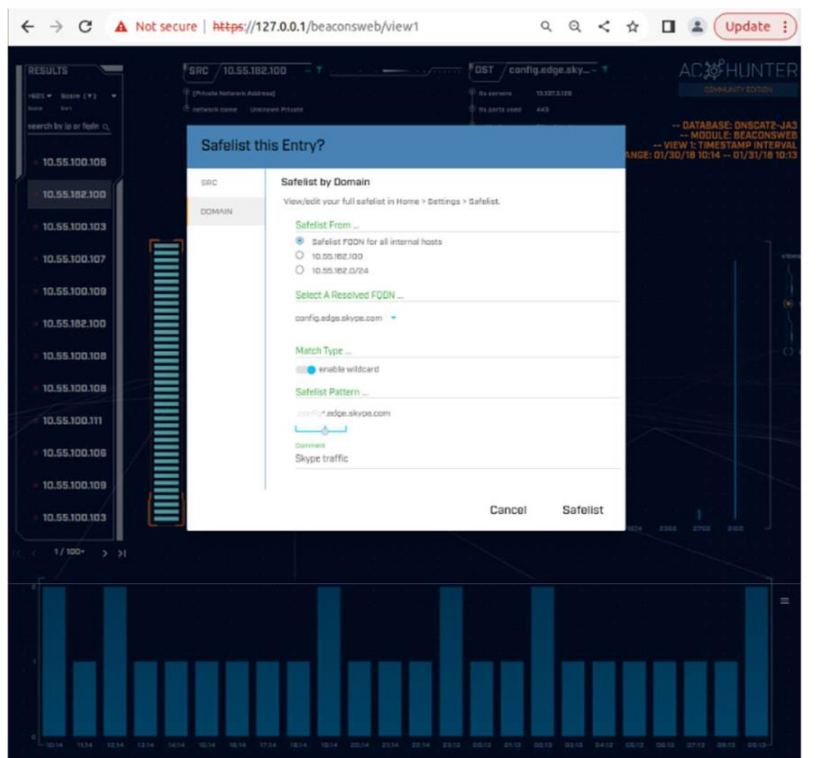
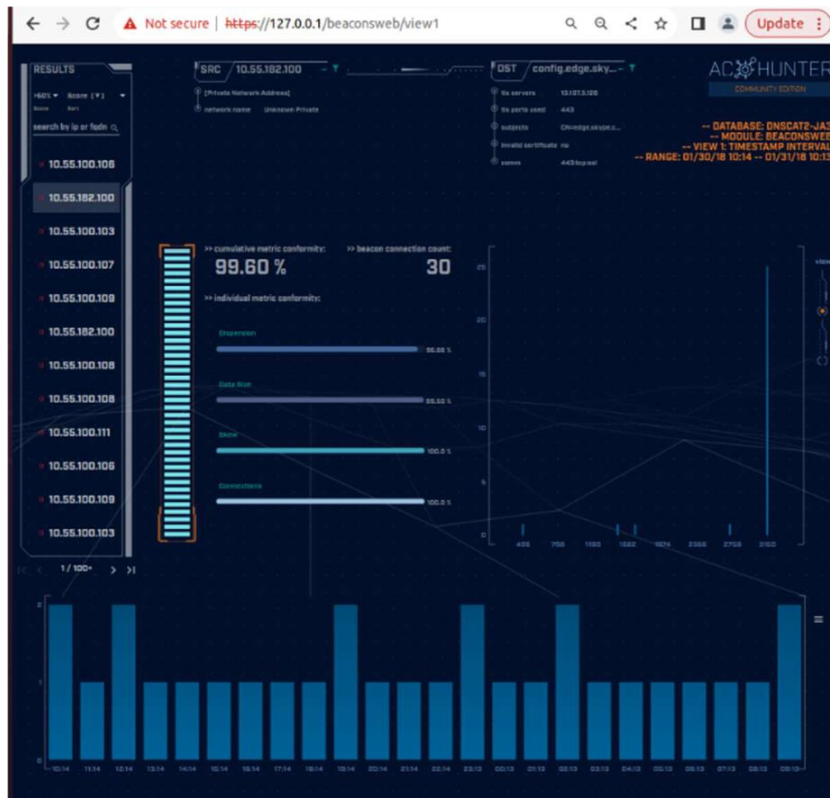
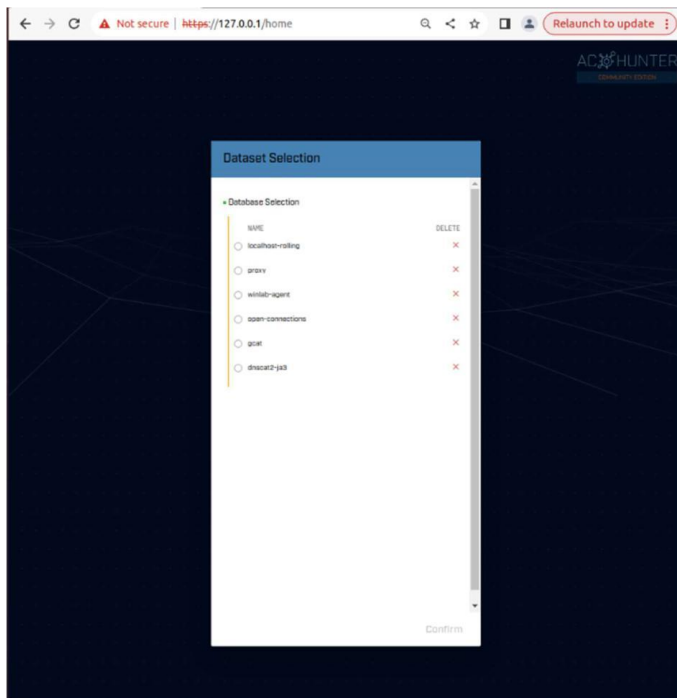
Скачиваем и разворачиваем стенд



Авторизируемся



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



2 POTENTIAL CS OVERLAPS CARED DETECTED

VIEW / EDIT GLOBAL SAFELIST

Global Safelist Entries

Search
Ex. 10.10.10.10

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

|< < 1/1 > >|

Close

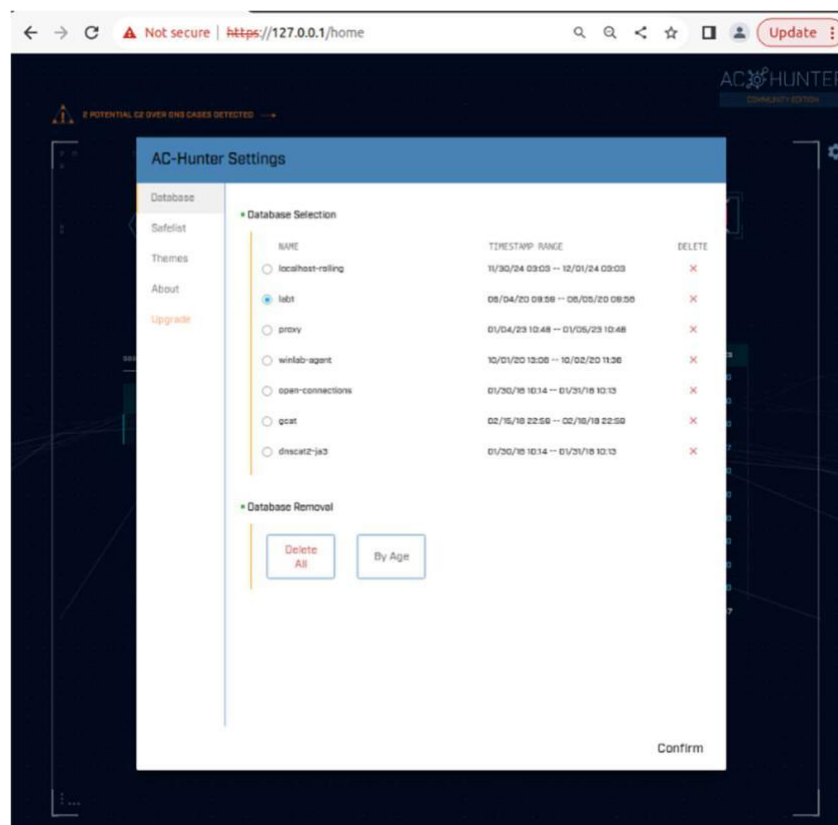
Lab 1

Импортируем логи и переключаемся на них в стенде

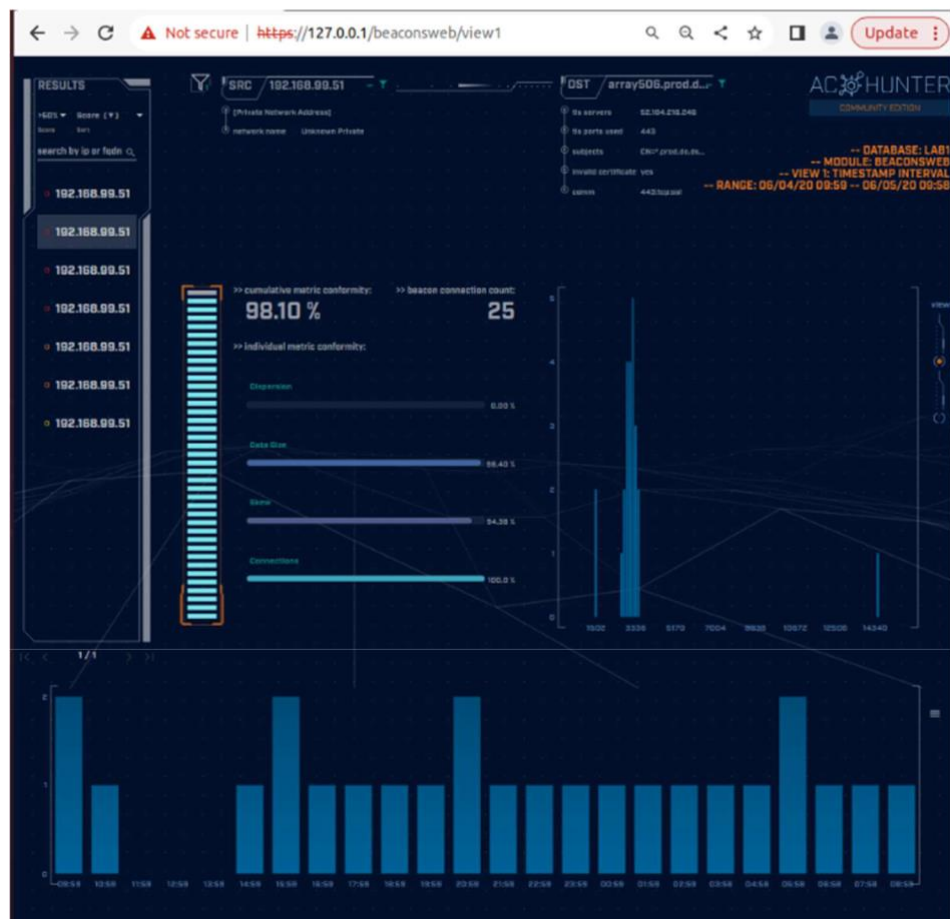
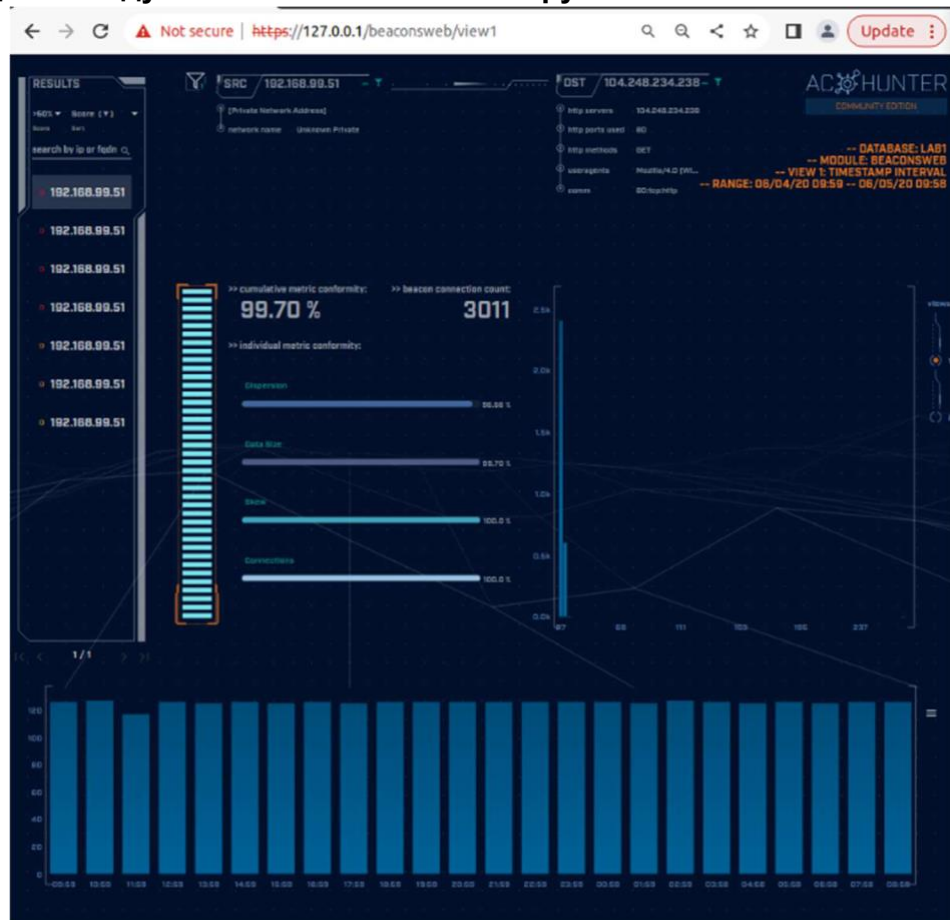
```
threat@ubuntu:~$ cd labs/lab
lab1/ lab2/ lab3/
threat@ubuntu:~$ cd labs/lab
lab1/ lab2/ lab3/
threat@ubuntu:~$ cd labs/lab1
threat@ubuntu:~/labs/lab1$ rita import *.log lab1
[sudo] password for threat:
Creating achunter_api_run ... done

[+] 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-а, когда зараженное устройство связывается с управляющим сервером (C2).

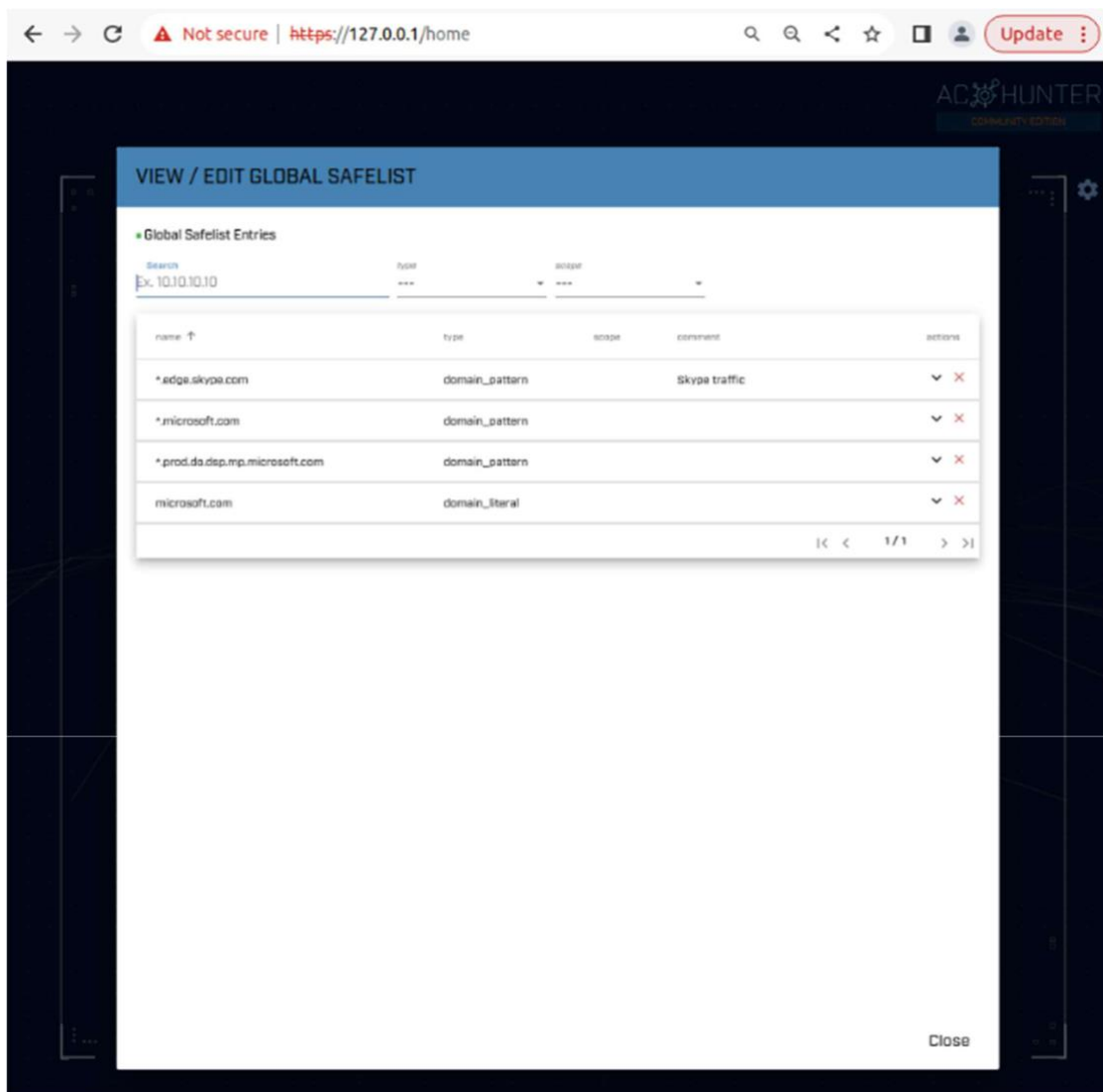
Общее количество соединений (3011):

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:

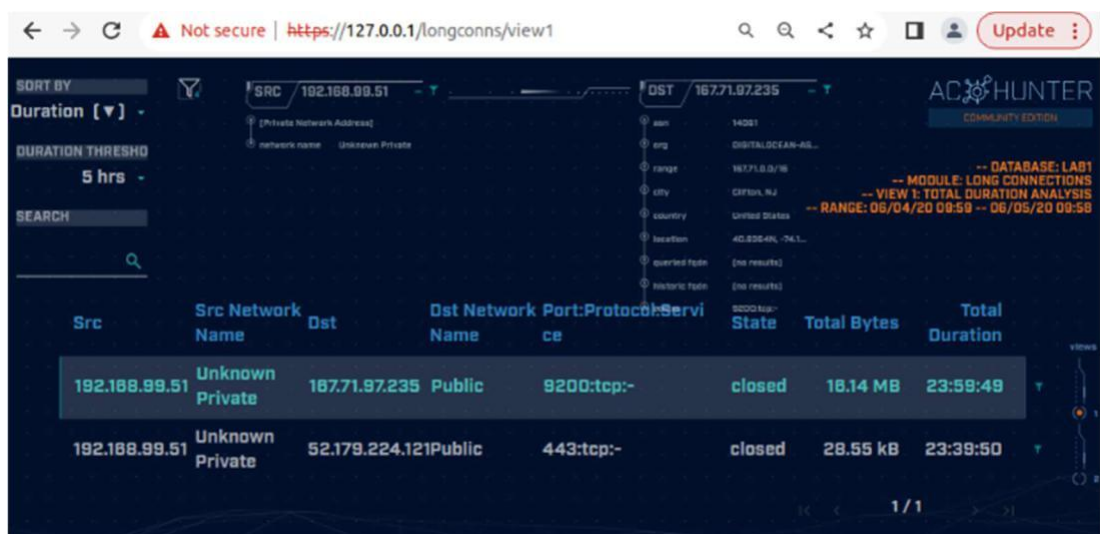
Использование HTTP без шифрования:

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

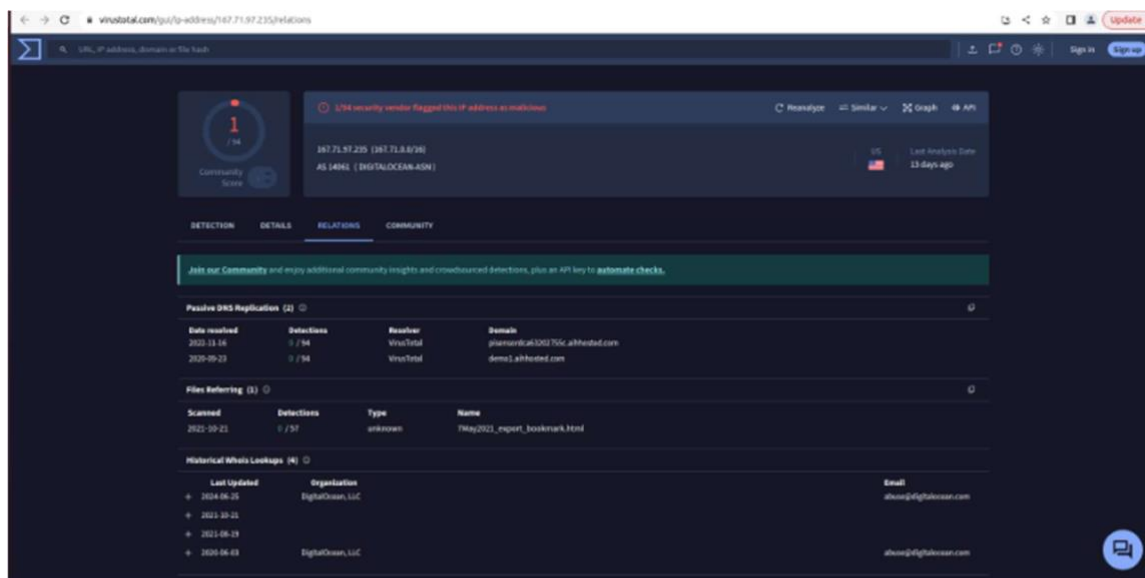
Практически все адреса связаны с Windows, так что добавляем их в safelist Конечный safelist



Перейдём в модуль длительных соединений



Всего 2 адреса, проверим их через VirusTotal



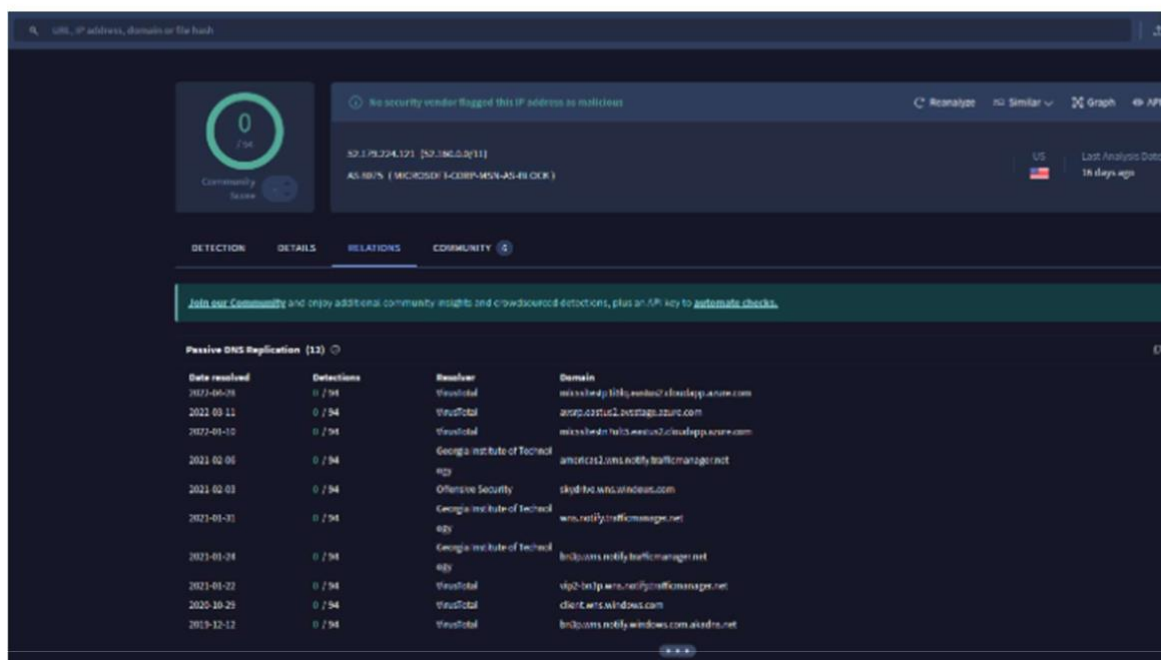
The screenshot shows the VirusTotal report for IP address 187.71.57.235. The interface is in dark mode. At the top, a green circle with the number '1' indicates a low community score. A warning message states: '1/54 security vendor flagged this IP address as malicious'. The IP is associated with AS 4861 (DIGITALOCEAN-ASN). Below the main header, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. A green banner encourages joining the community. The 'Positive DNS Replication' section shows two entries:

Date resolved	Detections	Resolver	Domain
2023-11-14	0 / 54	VirusTotal	piensorcad6302755c.aiihosted.com
2020-09-23	0 / 54	VirusTotal	demo1.aiihosted.com

The 'Files Referring' section shows one entry:

Scanned	Detections	Type	Name
2021-09-23	0 / 57	unknown	file/2021_report_bookmark.html

The 'Historical Whois Lookups' section shows four entries, all from DigitalOcean, LLC, with the email shaw@digitalocean.com.



The screenshot shows the VirusTotal report for IP address 32.178.224.121. The interface is in dark mode. At the top, a green circle with the number '0' indicates a low community score. A warning message states: 'No security vendor flagged this IP address as malicious'. The IP is associated with AS 8075 (MICROSOFT-CORP-MSN-AS-BLOCK). Below the main header, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. A green banner encourages joining the community. The 'Positive DNS Replication' section shows twelve entries:

Date resolved	Detections	Resolver	Domain
2023-06-06	0 / 54	VirusTotal	msxshdp1blywmdco7xibwappx.com
2022-09-11	0 / 54	VirusTotal	anpoc31uc2.mstags.mst.com
2022-09-10	0 / 54	VirusTotal	msxshdp1blywmdco7xibwappx.com
2021-02-06	0 / 54	Georgia Institute of Technol	amocic12.mst.mst.com
2021-02-03	0 / 54	Offensive Security	clpdt-fo.mst.mst.com
2021-01-31	0 / 54	Georgia Institute of Technol	www.mst.mst.com
2021-01-24	0 / 54	Georgia Institute of Technol	brdquams.mst.mst.com
2021-01-22	0 / 54	VirusTotal	vdp2-fo.mst.mst.com
2020-10-29	0 / 54	VirusTotal	client.mst.mst.com
2019-12-12	0 / 54	VirusTotal	brdquams.mst.mst.com

VirusTotal поместил один из адресов, как вредоносный.

Подозрительная природа доменов Связанные с IP домены piensorcad6302755c.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.

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 09:56	✖
<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 11:36	✖
<input type="radio"/> open-connections	01/30/16 10:14 -- 01/31/16 10:13	✖
<input type="radio"/> qcat	02/16/16 22:56 -- 02/16/16 22:56	✖
<input type="radio"/> dnscat2-jas	01/30/16 10:14 -- 01/31/16 10:13	✖

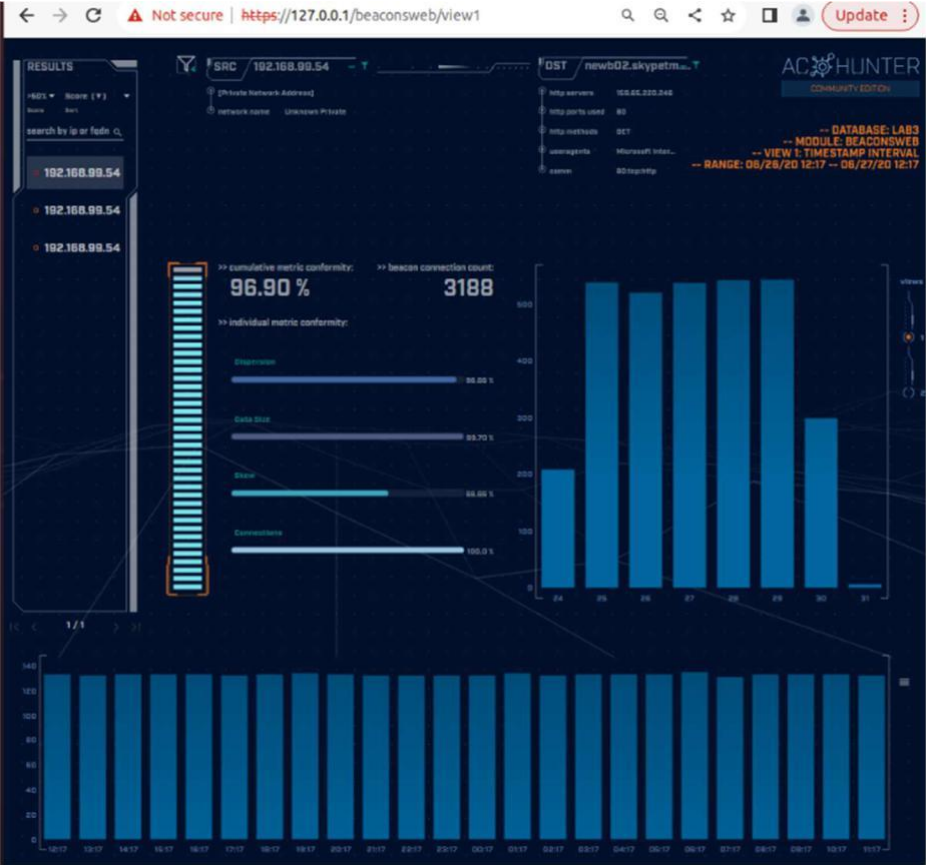
* Database Removal

Delete All

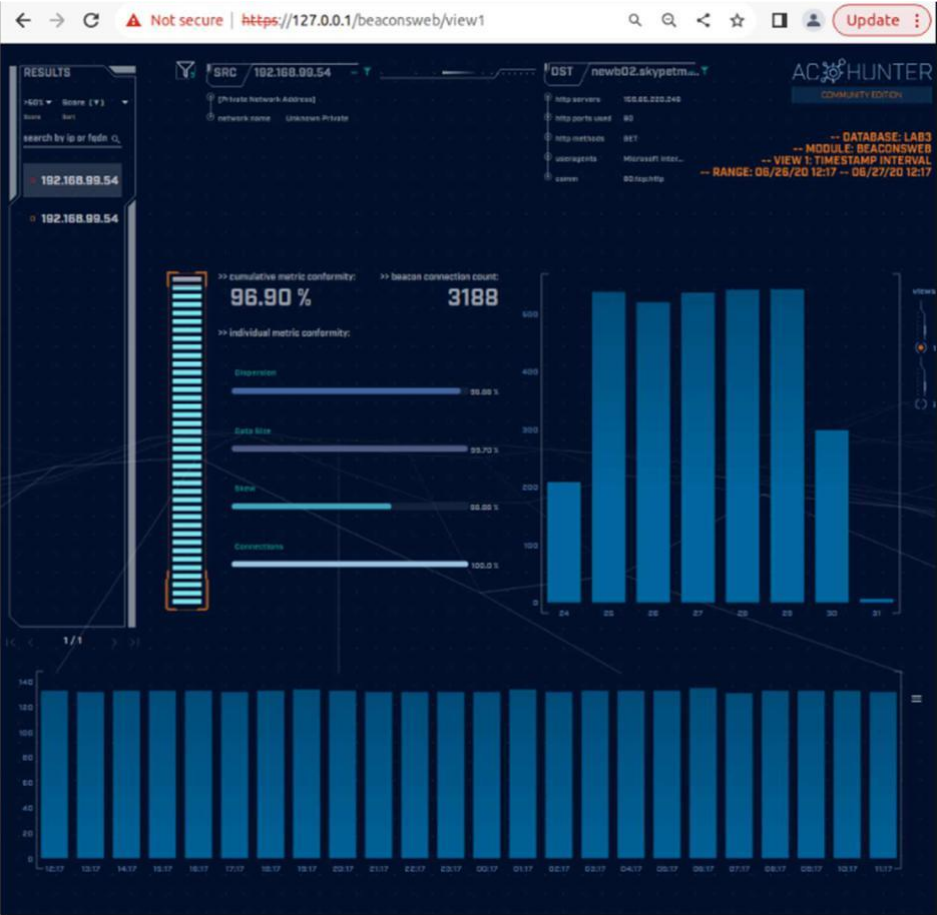
By Age

Confirm

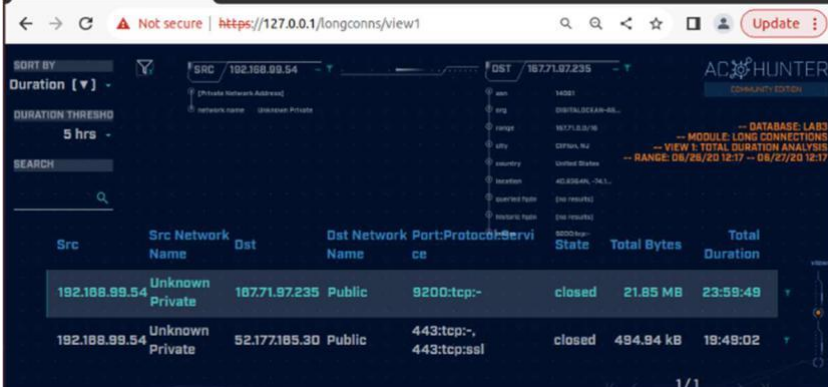
Переходим в модуль beacons web



Анализируем адреса и вносим легитивные в safelist



Остается всего два адреса, проверим каждый через VirusTotal



The screenshot shows the ACX Hunter web interface. The top navigation bar includes a search bar, filters for source and destination IP addresses, and a table of connection details. The table has columns for Src, Src Network Name, Dst, Dst Network Name, Port:Protocol:Service, Status, Total Bytes, and Total Duration. Two connections are listed:

Src	Src Network Name	Dst	Dst Network Name	Port:Protocol:Service	Status	Total Bytes	Total Duration
192.168.99.54	Unknown Private	107.71.97.235	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	19:48:02

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.