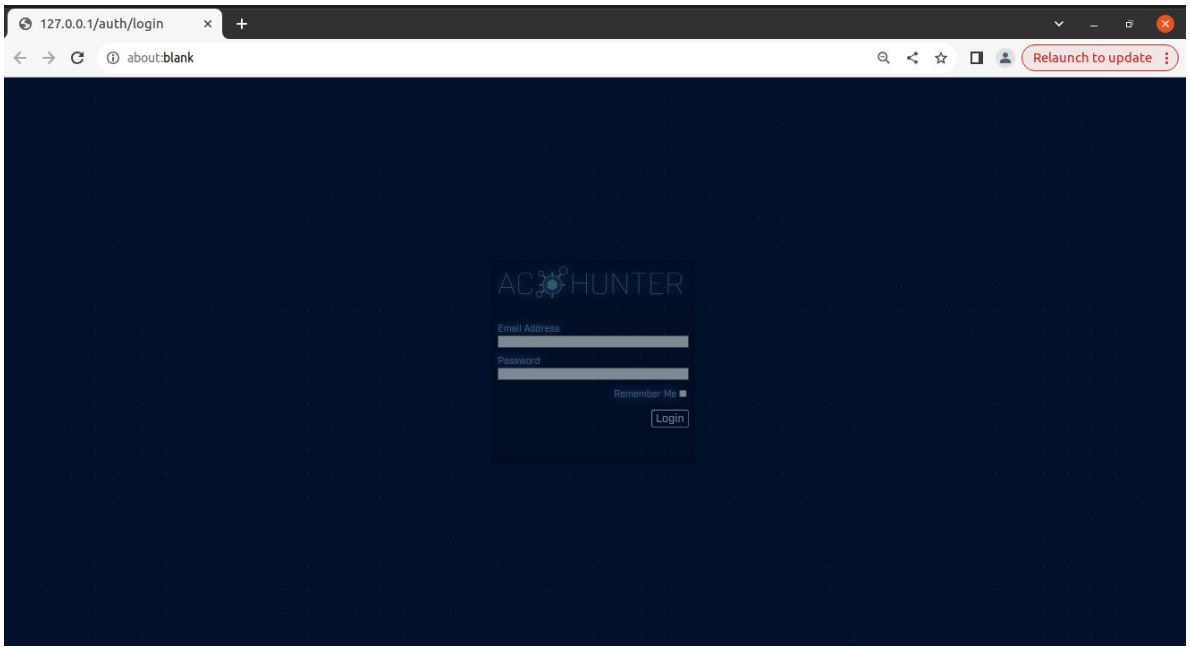
Практическая работа № 4: Network Threat Hunting

Выполнил Ионов Максим Сергеевич, группа ББМО-02-23

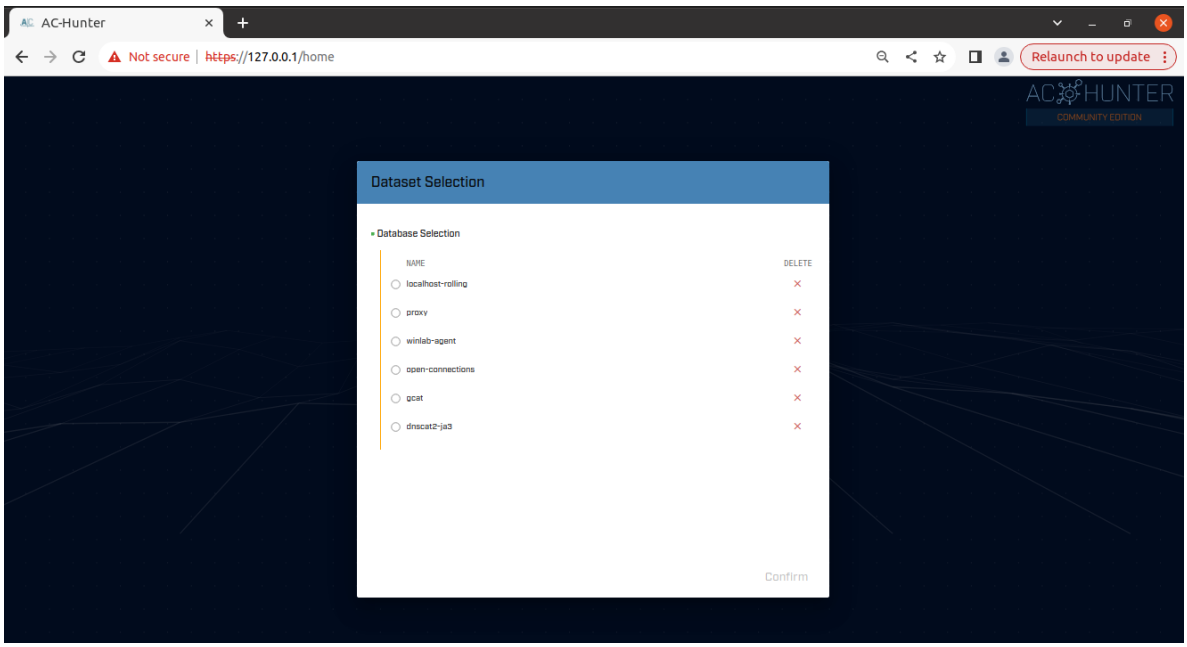
Ход работы

Первый набор данных

1) Поднимаем виртуальную машину из заранее заготовленного образа.
   После запуска виртуальной машины заходим в браузер и видим приветственное окно



2) Используем полученные данные и входим в учетную запись. После входа выбираем датасет с которым мы будем работать

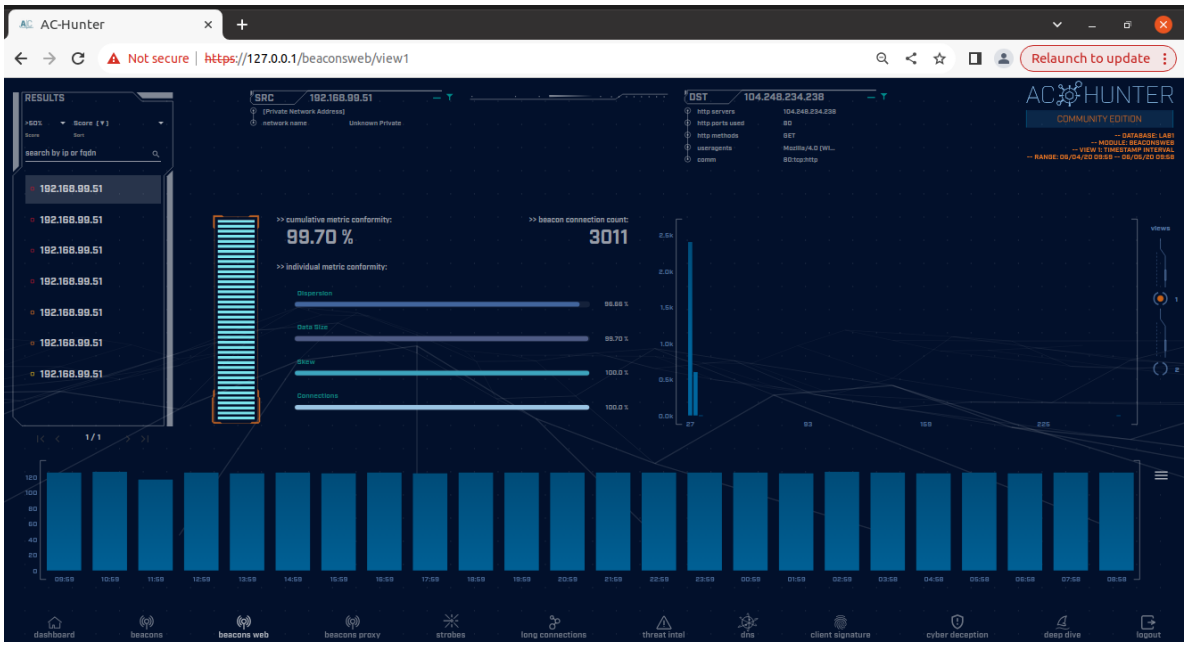


3) В системе уже хранятся готовые датасеты с которыми мы будем работать (lab1, lab2, lab3). Загружаем первый датасет

```
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.l
og /home/threat/labs/lab1/http.log /home/threat/labs/lab1/known_hosts.log /home/threat/labs/la
b1/known_services.log /home/threat/labs/lab1/loaded_scripts.log /home/threat/labs/lab1/notice.
log /home/threat/labs/lab1/ntp.log /home/threat/labs/lab1/packet_filter.log /home/threat/labs/
lab1/software.log /home/threat/labs/lab1/ssl.log /home/threat/labs/lab1/stats.log /home/threat
/labs/lab1/x509.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 155ms
        [-] 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 ...
```

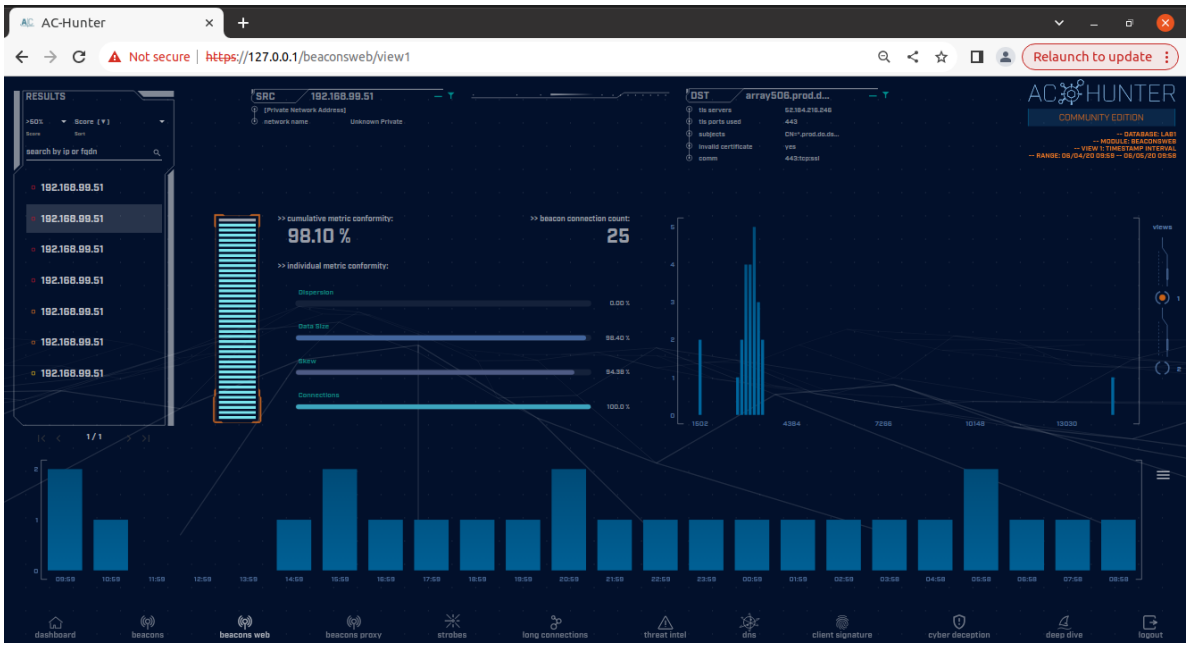
4) После загрузки выбираем его и нам открывается рабочая панель с нашими данными



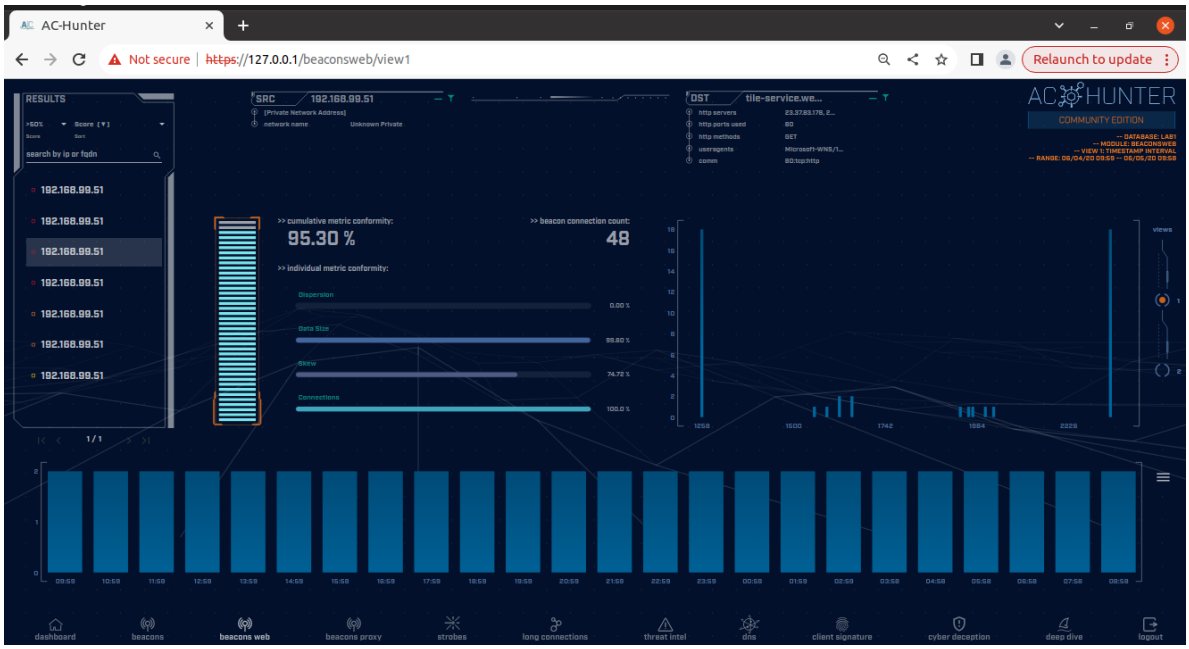
5) Начнем анализировать наши данные

5.1) Первая запись: Значение beacon score очень высокое, пользовательский агент определился как Windows 7, за последний день наблюдается большое количество подключений, отсутствует строка хостинг

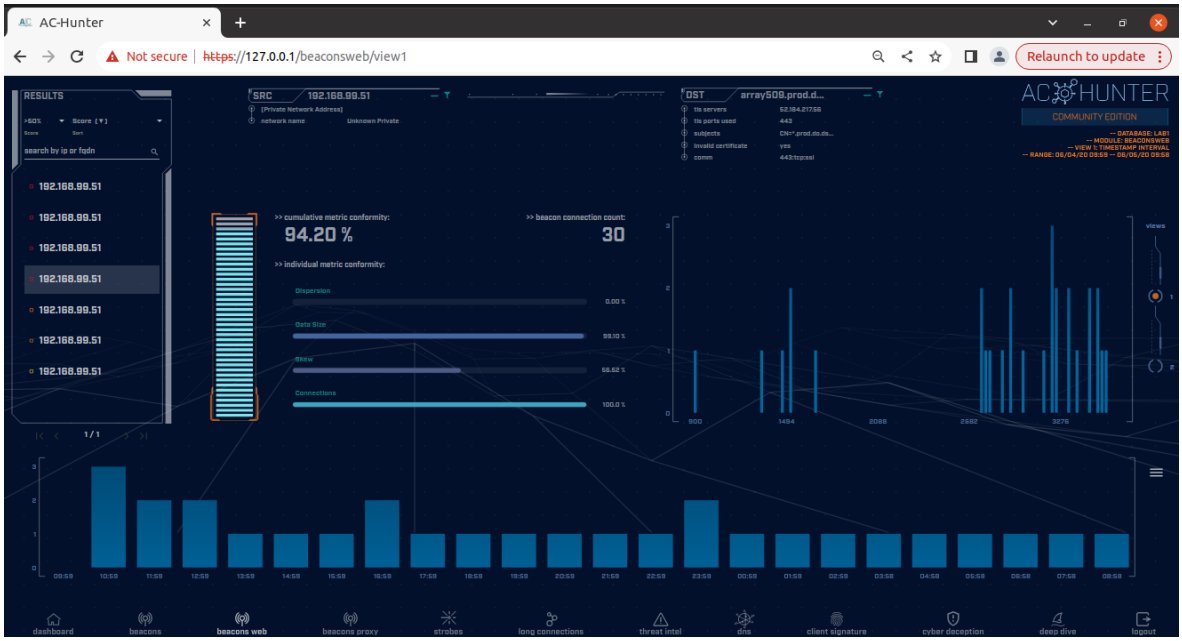
5.2) Вторая запись: Значение beacon низкое, есть легитимный сертификат, анализ в гугле показал что данная запись принадлежит Windows и считается легитимной



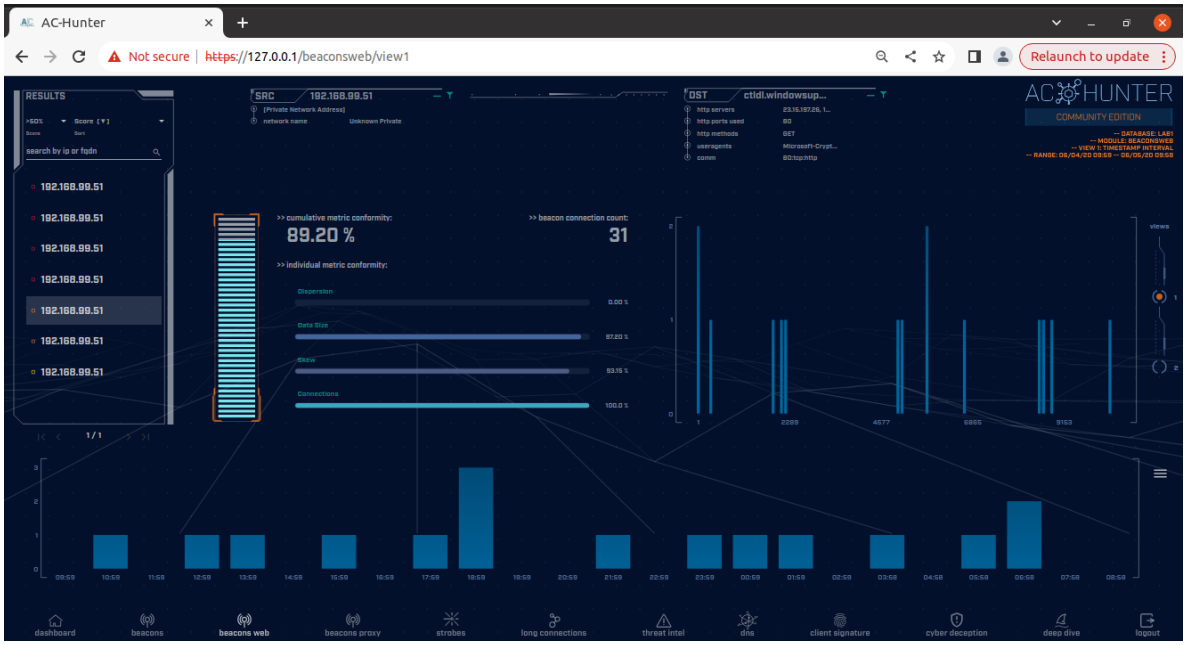
5.3) Третья запись: Значение beacon низкое, принадлежит Wts (Windows tile services)



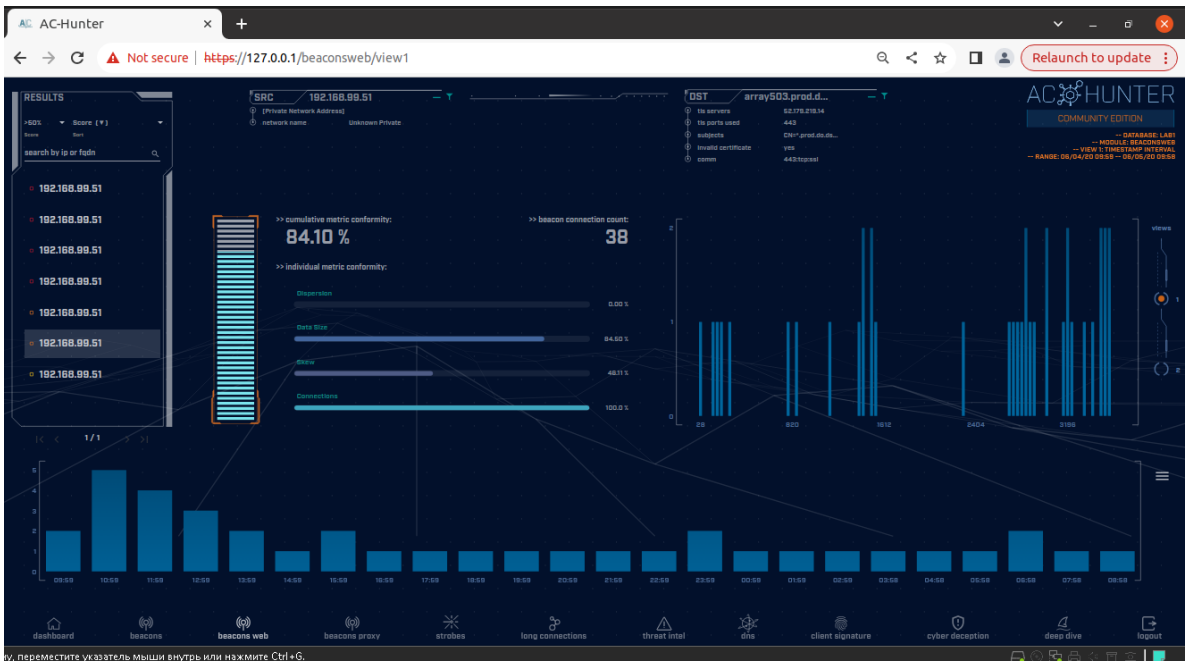
5.4) Четвертая запись: Значение beacon низкое, имеет схожесть со второй записью



5.5) Пятая запись: Значение beacon низкое, имеет схожесть с предыдущими записями

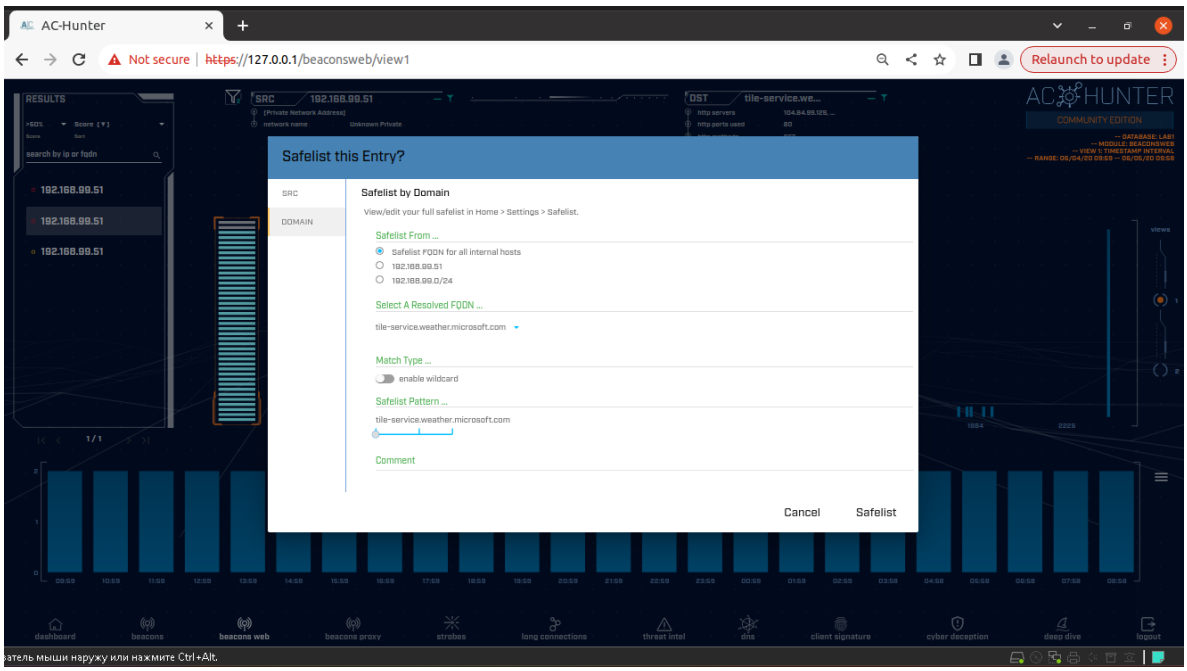


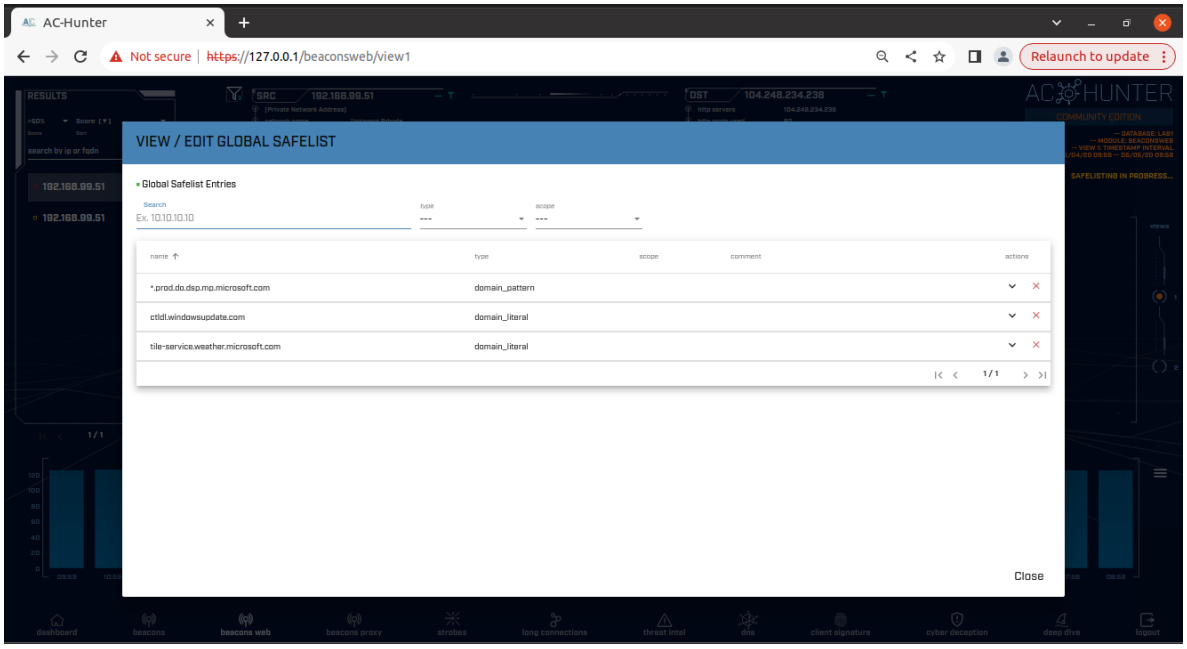
5.6) Шестая запись: Значение beacon низкое, имеет сходство с четвертой записью

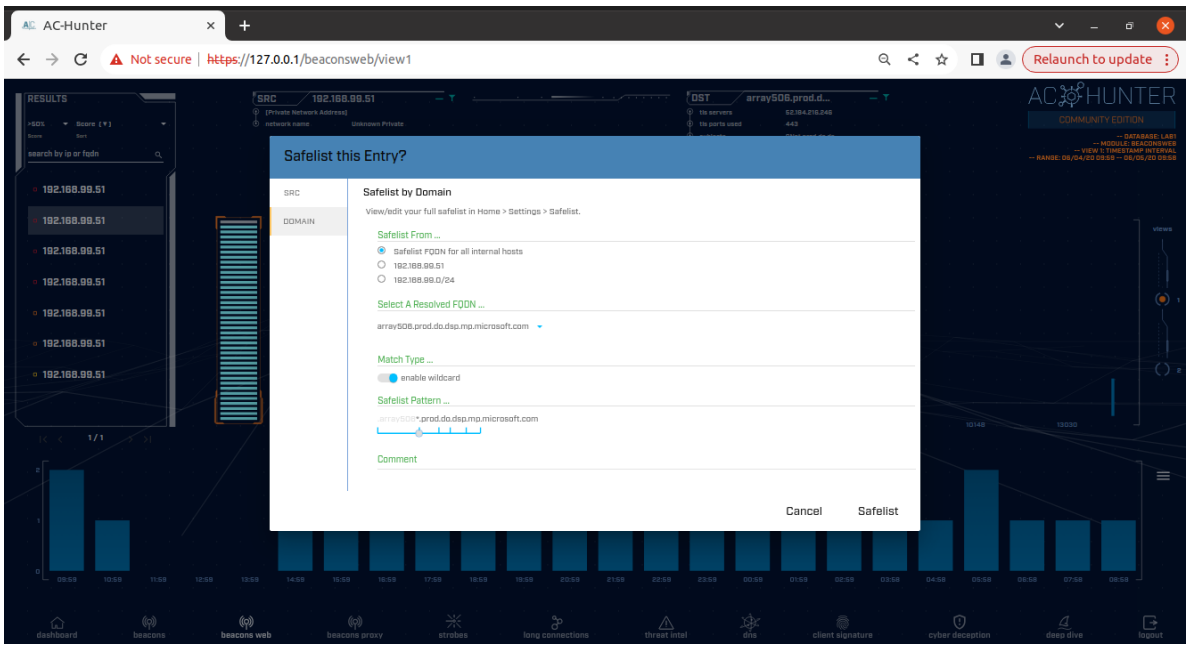


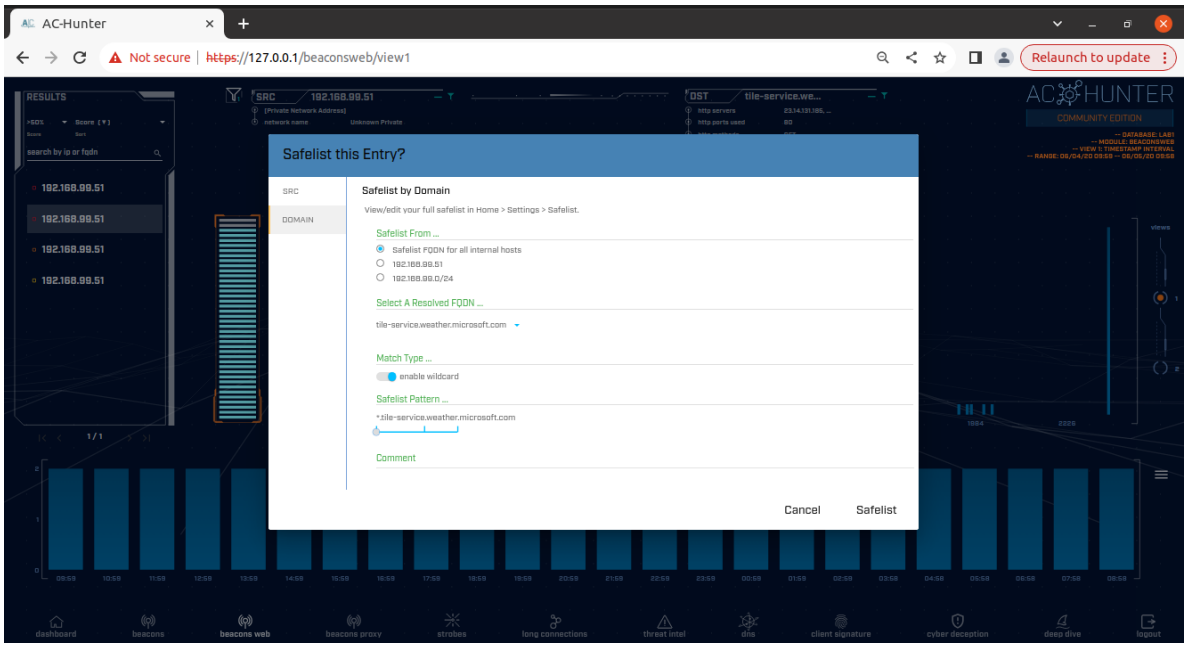
6) после анализа записей стало ясно что первая выглядит довольно подозрительно и требует детального анализа, оставшиеся записи относятся к службам Windows

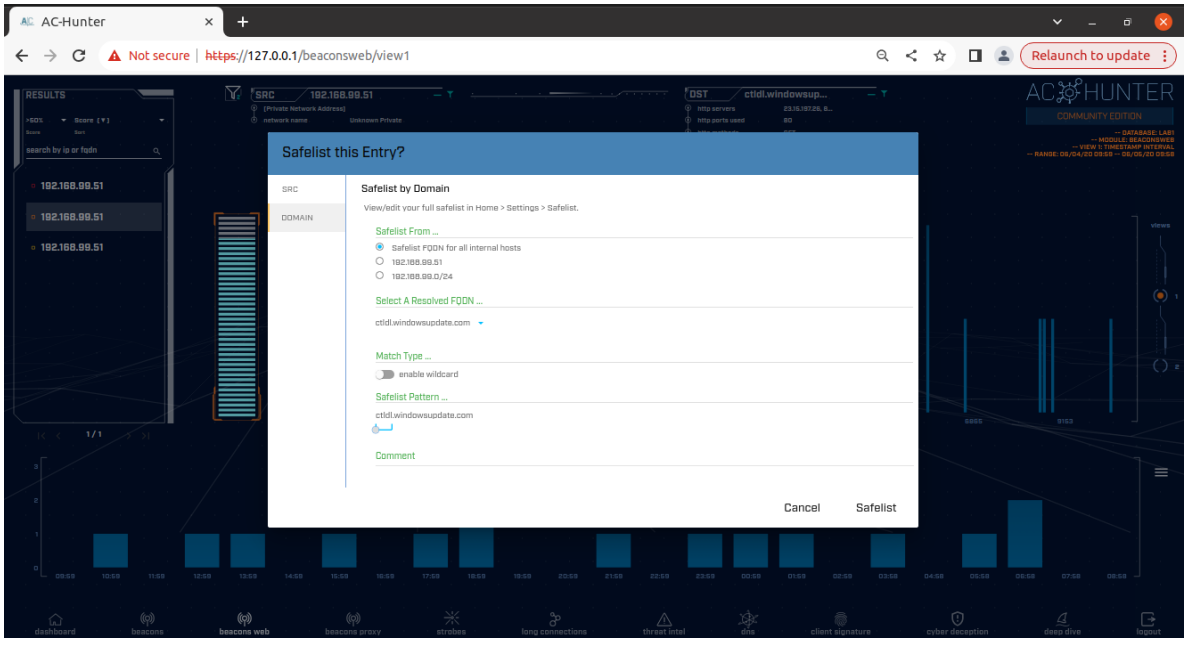
7) Для дальнейшего анализа внесем легитимные на наш взгляд записи в safelist


AC-Hunter
Not secure | https://127.0.0.1/beaconsweb/view1
Relaunch to update
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
192.168.99.51
192.168.99.0/24
Select A Resolved FQDN ...
tile-service.weather.microsoft.com
Match Type ...
enable wildcard
Safelist Pattern ...
tile-service.weather.microsoft.com
Comment
Cancel
Safelist
dashboard
beacons
beacons web
beacons proxy
strobes
long connections
threat intel
dns
client signature
cyber deception
deep dive
logout

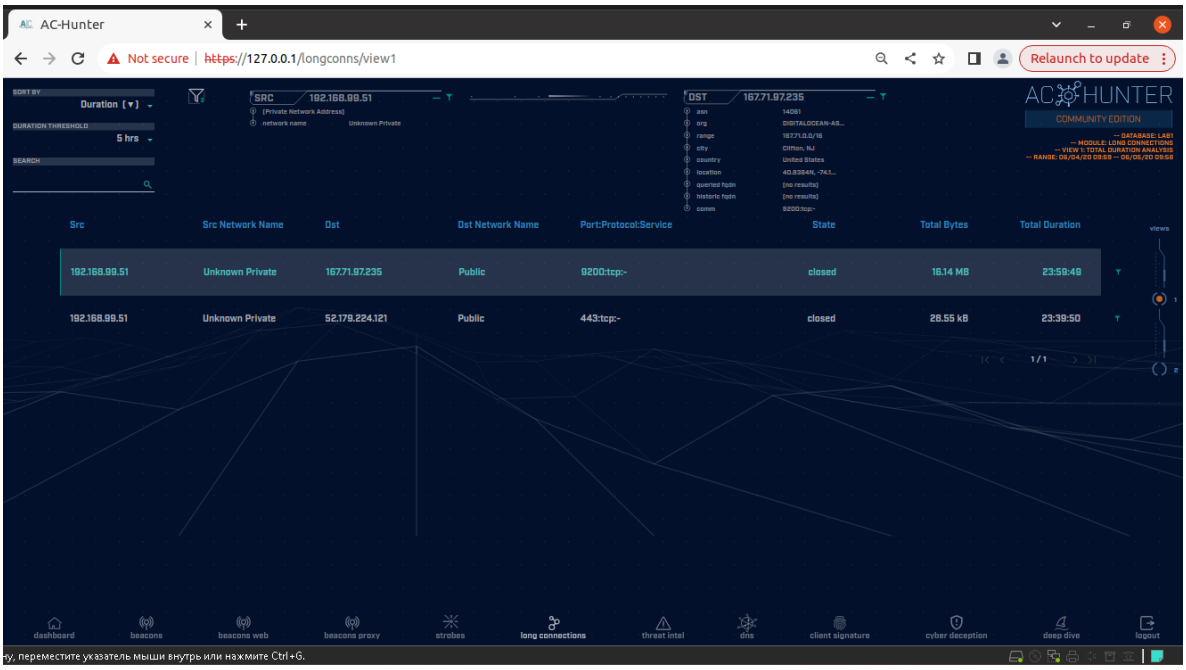

AC-Hunter
Not secure | https://127.0.0.1/beaconsweb/view1
Relaunch to update
VIEW / EDIT GLOBAL SAFELIST
Global Safelist Entries
Search
Ex. 10.10.10.10
type
scope
name
type
scope
comment
actions
*.prod.do.dsp.mp.microsoft.com
domain_pattern
ctldl.windowsupdate.com
domain_literal
tile-service.weather.microsoft.com
domain_literal
1 / 1
Close
dashboard
beacons
beacons web
beacons proxy
strobes
long connections
threat intel
dns
client signature
cyber deception
deep dive
logout


AC-Hunter
Not secure | https://127.0.0.1/beaconsweb/view1
Relaunch to update
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
192.168.99.51
192.168.99.0/24
Select A Resolved FQDN ...
array506.prod.do.dsp.mp.microsoft.com
Match Type ...
enable wildcard
Safelist Pattern ...
array506*.prod.do.dsp.mp.microsoft.com
Comment
Cancel
Safelist


AC-Hunter
Not secure | https://127.0.0.1/beaconsweb/view1
Relaunch to update
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
192.168.99.51
192.168.99.0/24
Select A Resolved FQDN ...
tile-service.weather.microsoft.com
Match Type ...
enable wildcard
Safelist Pattern ...
*.tile-service.weather.microsoft.com
Comment
Cancel
Safelist

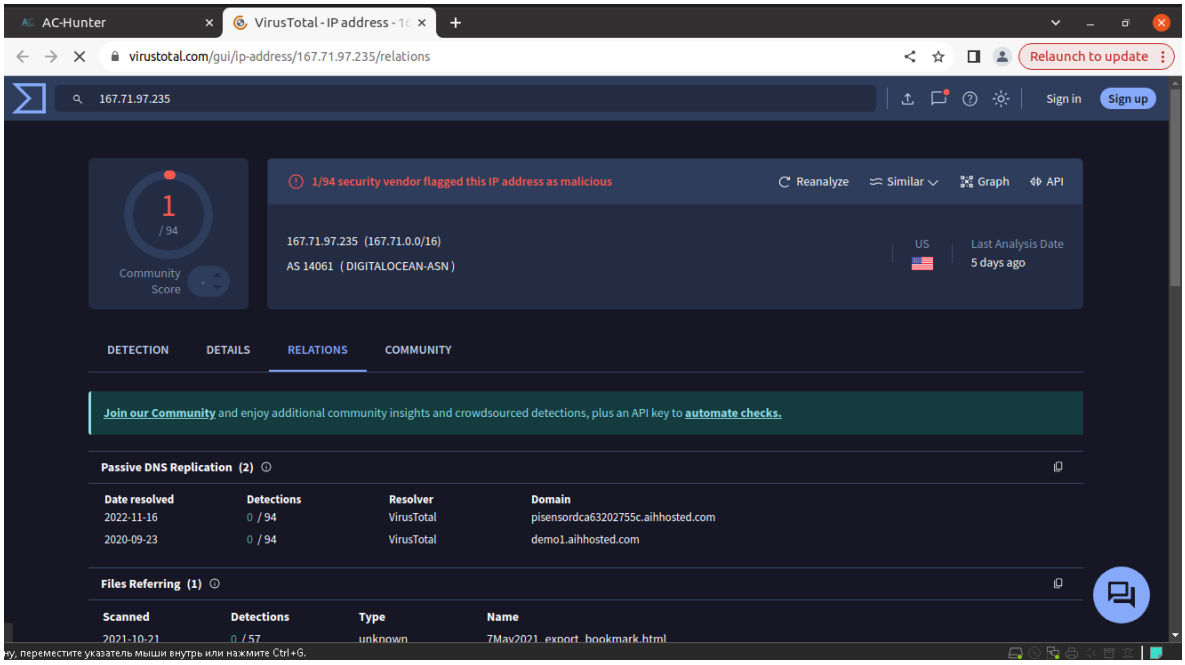

AC-Hunter
Not secure | https://127.0.0.1/beaconsweb/view1
Relaunch to update
Safelist this Entry?
SRC
DOMAIN
Safelist by Domain
View/edit your full safelist in Home > Settings > Safelist.
Safelist From ...
Safelist FQDN for all internal hosts
192.168.99.51
192.168.99.0/24
Select A Resolved FQDN ...
ctldl.windowsupdate.com
Match Type ...
enable wildcard
Safelist Pattern ...
ctldl.windowsupdate.com
Comment
Cancel
Safelist

8) После внесения в safelist перейдем во вкладку длительные подключения и начнем анализировать

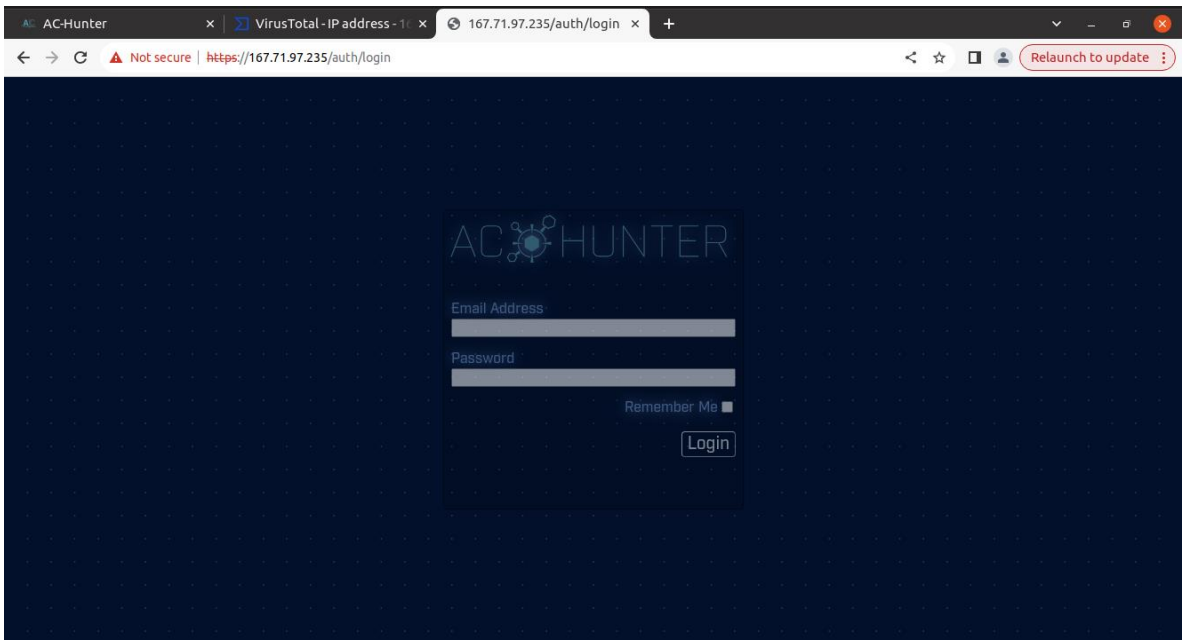


9) Видим 2 записи каждая из которых имеет продолжительность почти сутки. Проанализируем их через Virustotal

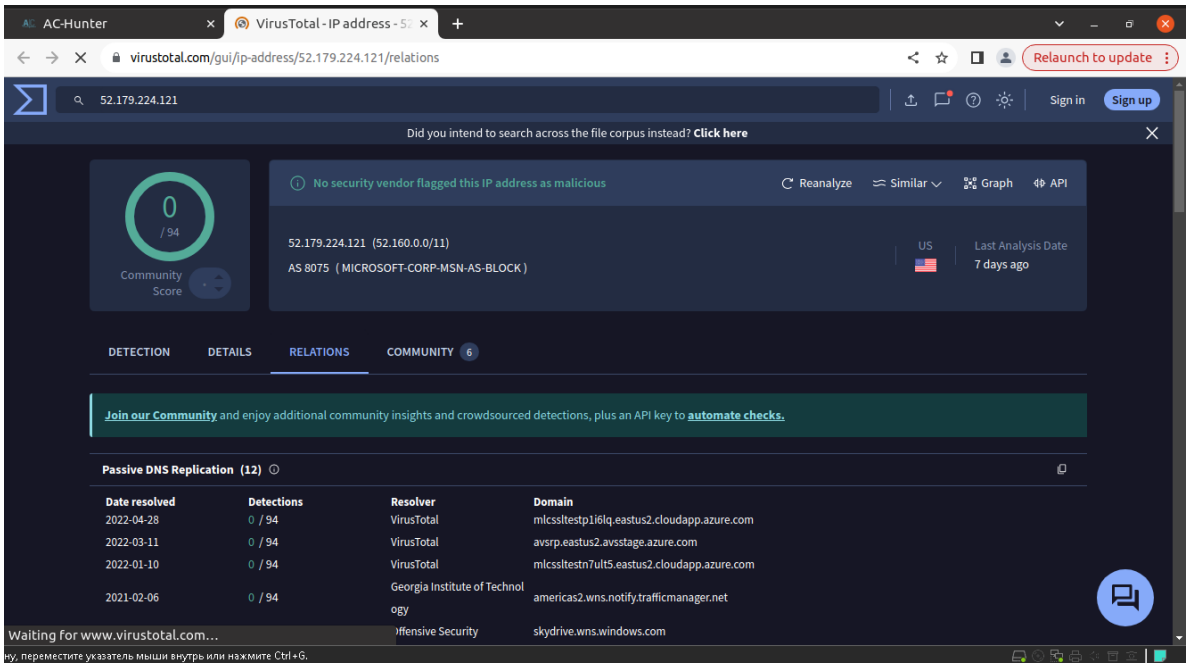
10) Открыв первую запись, видим сразу предупреждение об этом IP



11) Перейдя по этому адресу видим такое же приветственное окно как и у нас

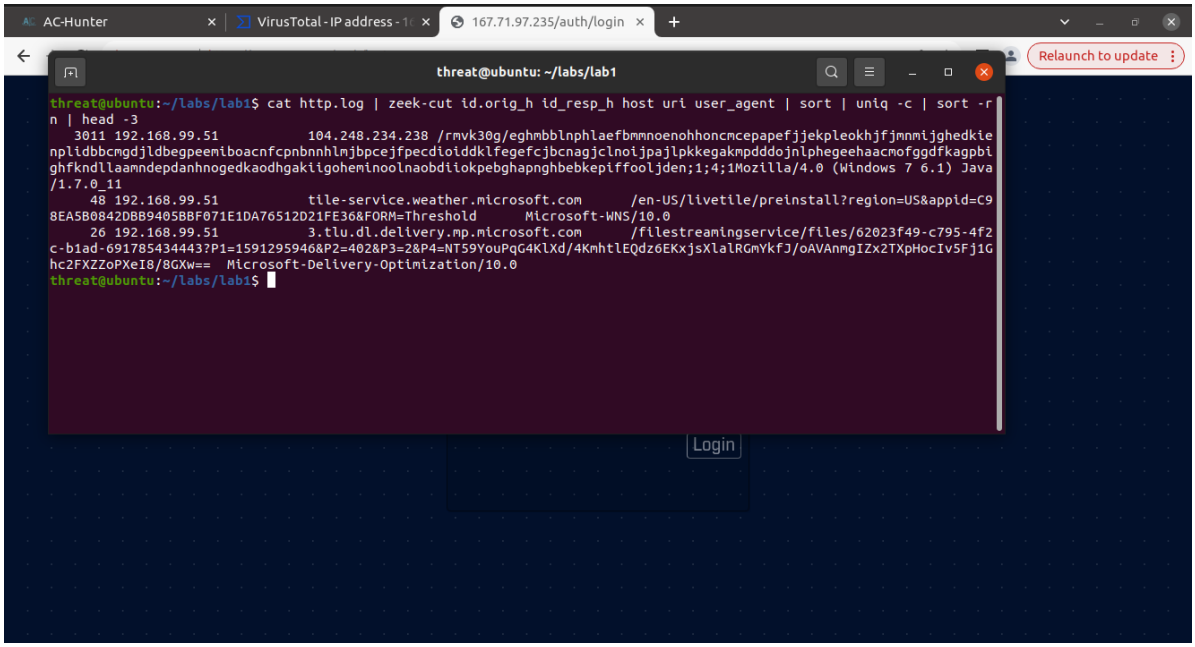


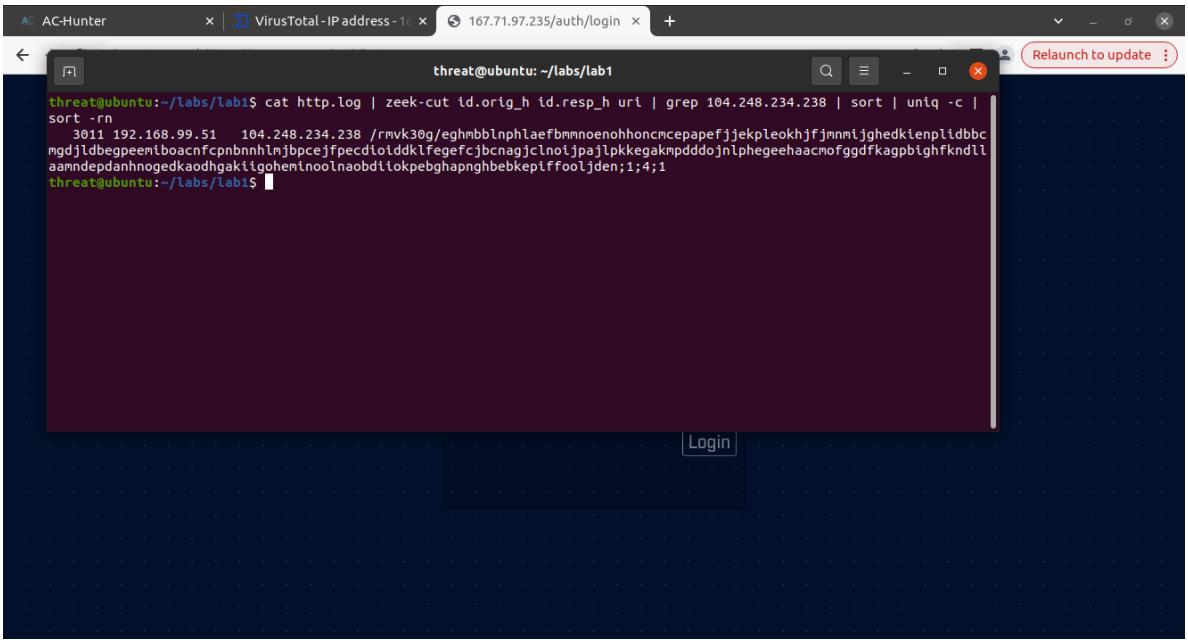
12) Открыв вторую запись видим что данный IP адрес легитимный



13) Следующим этапом посмотрим логи связанные с данной записью и ip адрессом

```
threat@ubuntu:~/labs/lab1$ cat http.log | zeek-cut id.orig_h id_resp_h host uri user_agent | sort | uniq | cut -f 3 |
 sort | uniq -c |  sort -rn
     31 ctldl.windowsupdate.com
      4 dl.delivery.mp.microsoft.com
      3 ocsp.digicert.com
      3 2.tlu.dl.delivery.mp.microsoft.com
      3 11.tlu.dl.delivery.mp.microsoft.com
      2 3.tlu.dl.delivery.mp.microsoft.com
      1 tile-service.weather.microsoft.com
      1 ocsp.msocsp.com
      1 adl.windows.com
      1 104.248.234.238
```





Проведя весь анализ, мы получили следующую информацию:

a) Количество соединений: 3011

b) Строка агента пользователя была подвержена изменению

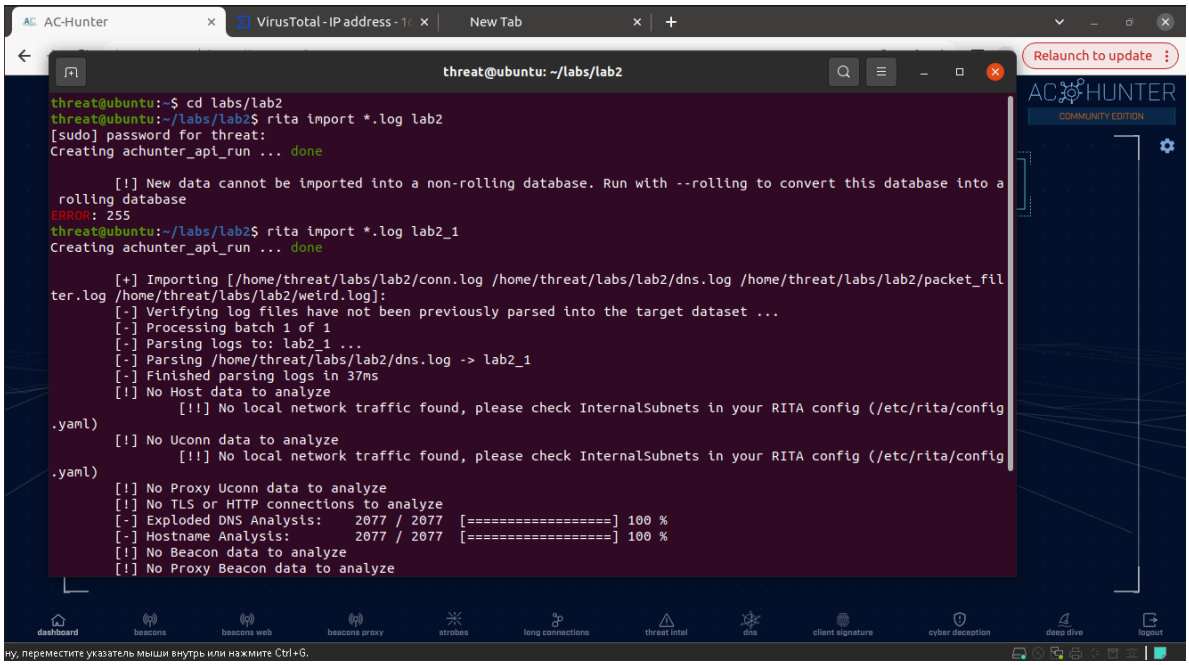
c) Отсутствие поля "host"

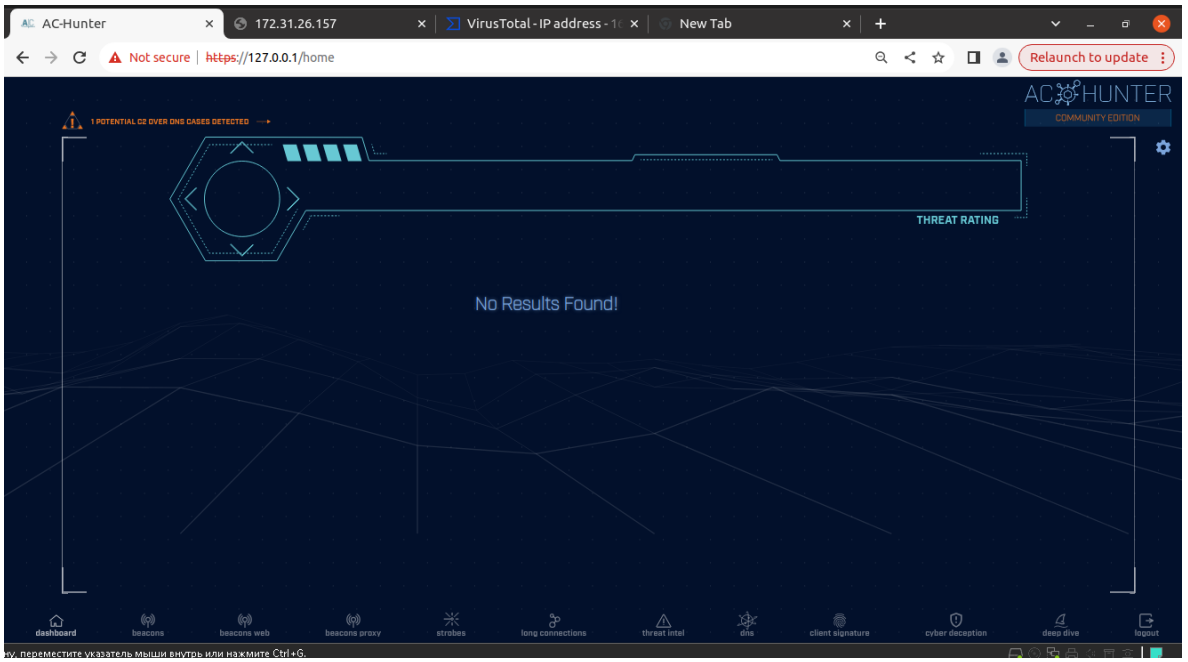
d) Строка URI имеет длинный и запутанный вид

Вывод: Соединения 104.248.234.238 явно является нелегитимным

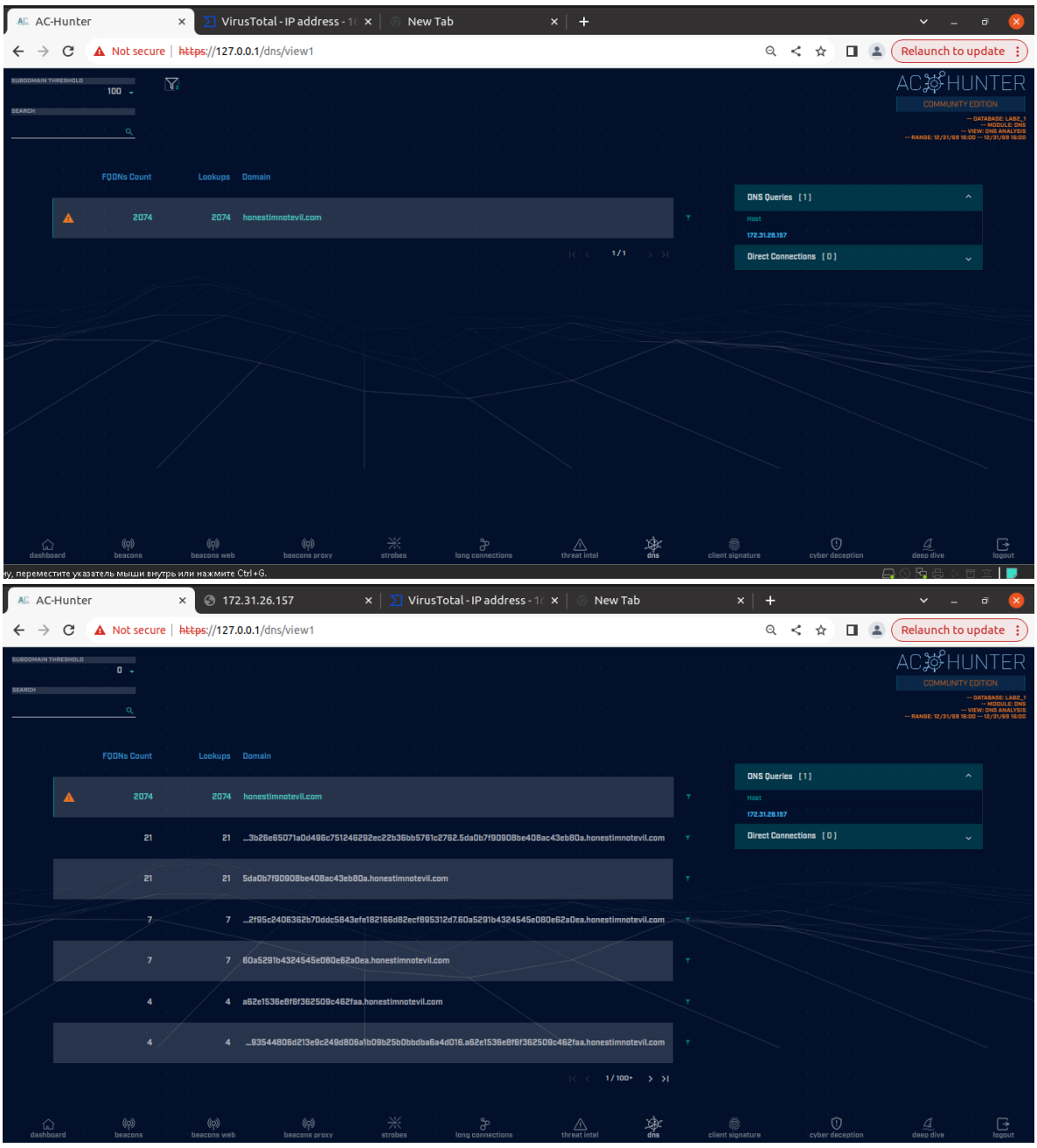
Второй набор данных

1) Загружаем второй набор данный. После загрузки система сразу нас предупреждает что возможно C2 через DNS





2) Открываем вкладку DNS для анализа



Проведя весь анализ, мы получили следующую информацию:

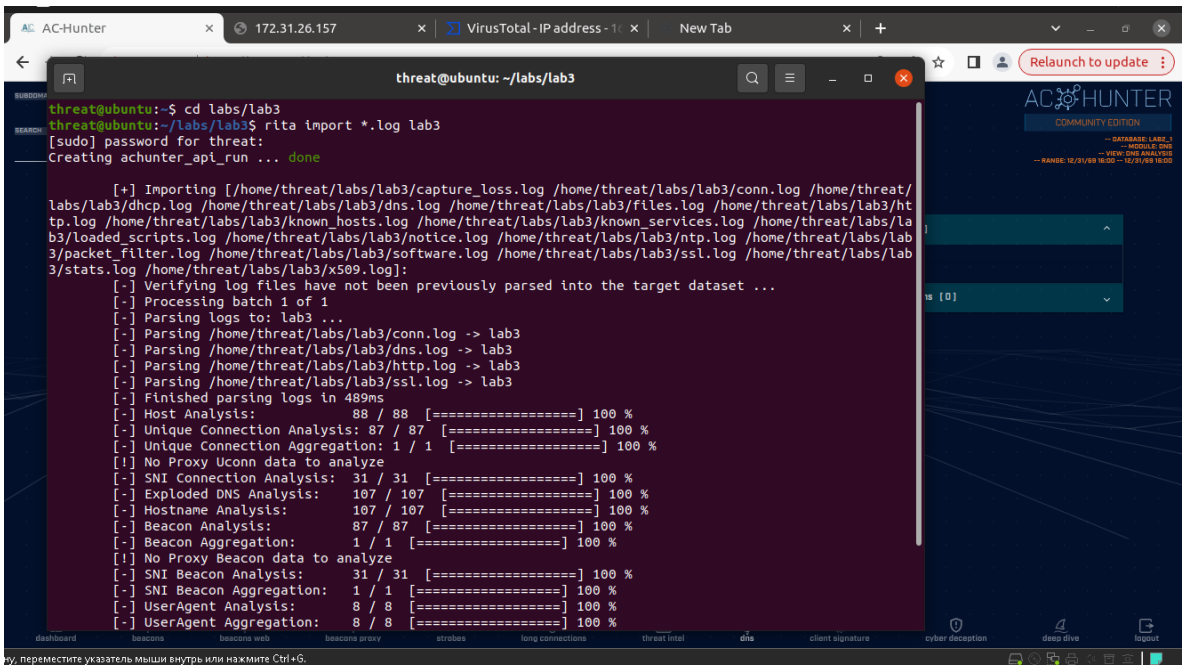
a) Возможно, C2 через DNS

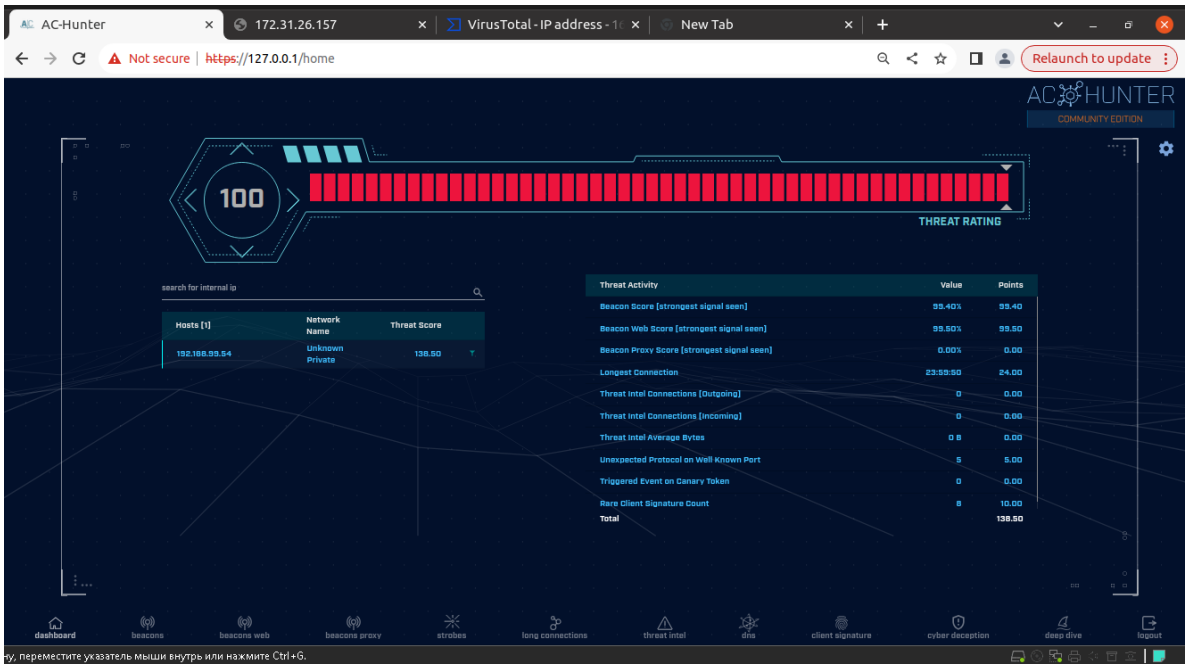
b) Имя хоста состоит из шестнадцатеричных символов

c) Отсутствие отдельных IP адресов

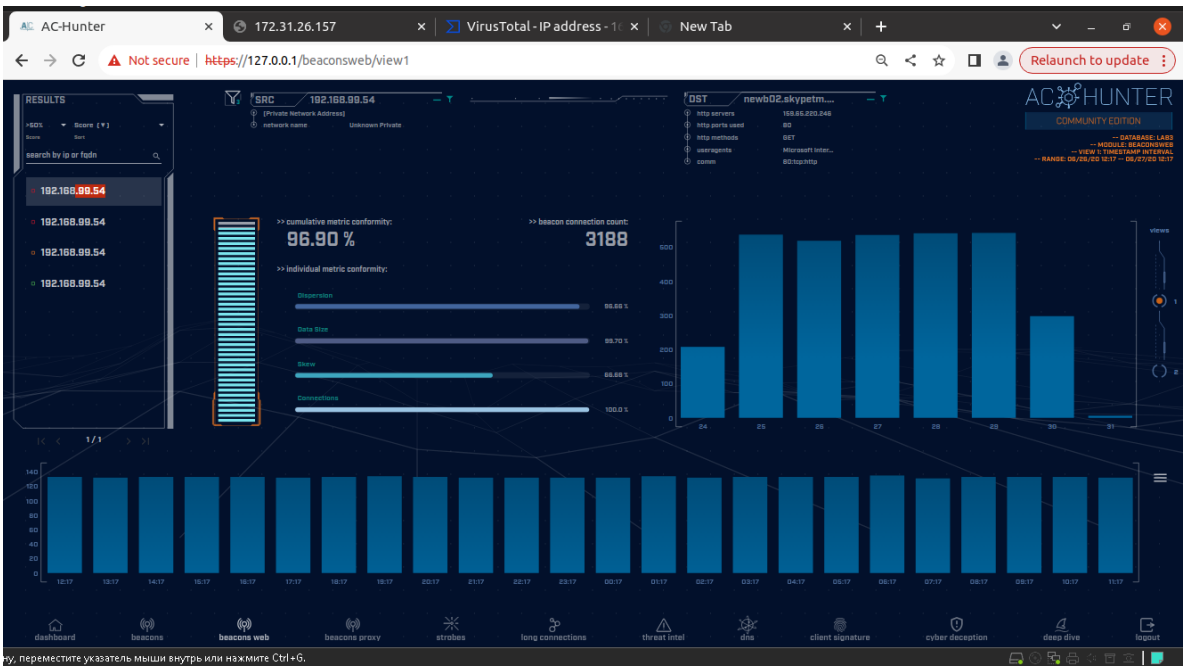
Третий набор данных

1) Загружаем третий набор данный. И сразу можем увидеть, что рейтинг равняется 100



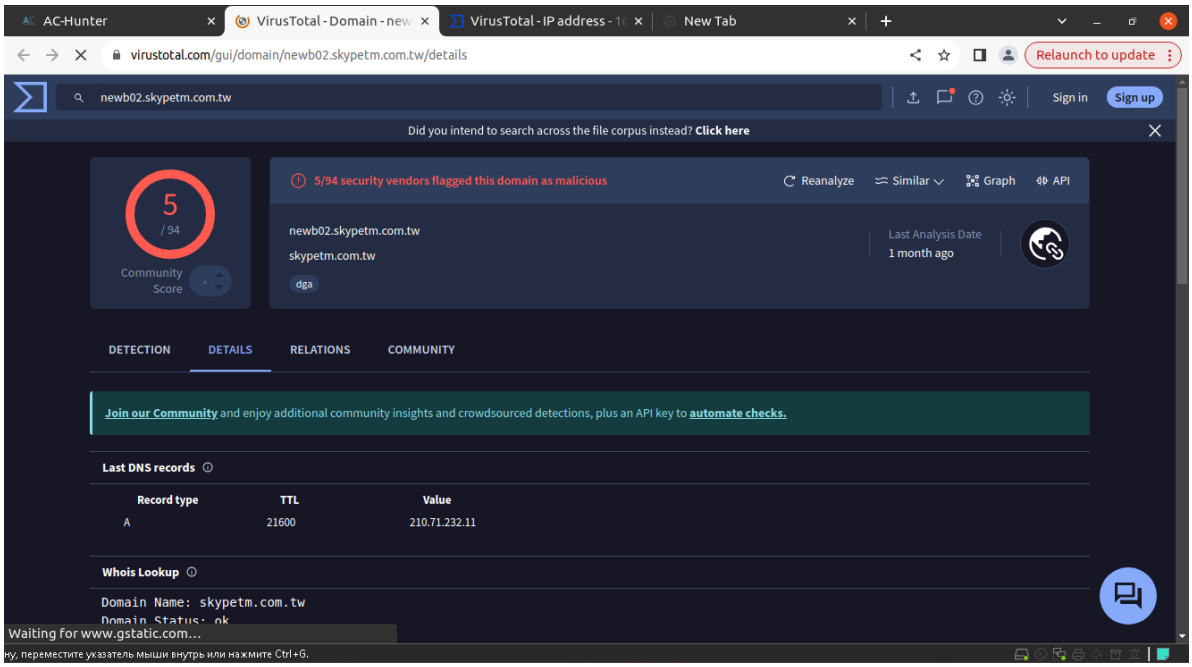


2) Переходим в раздел beacons web для анализа

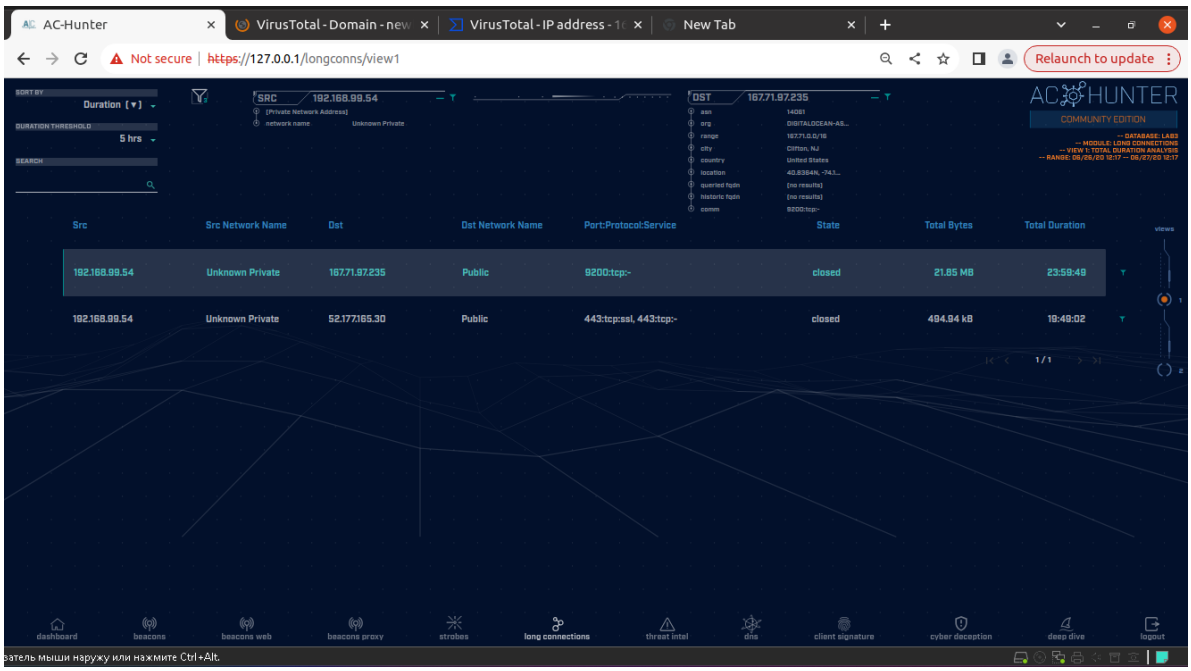


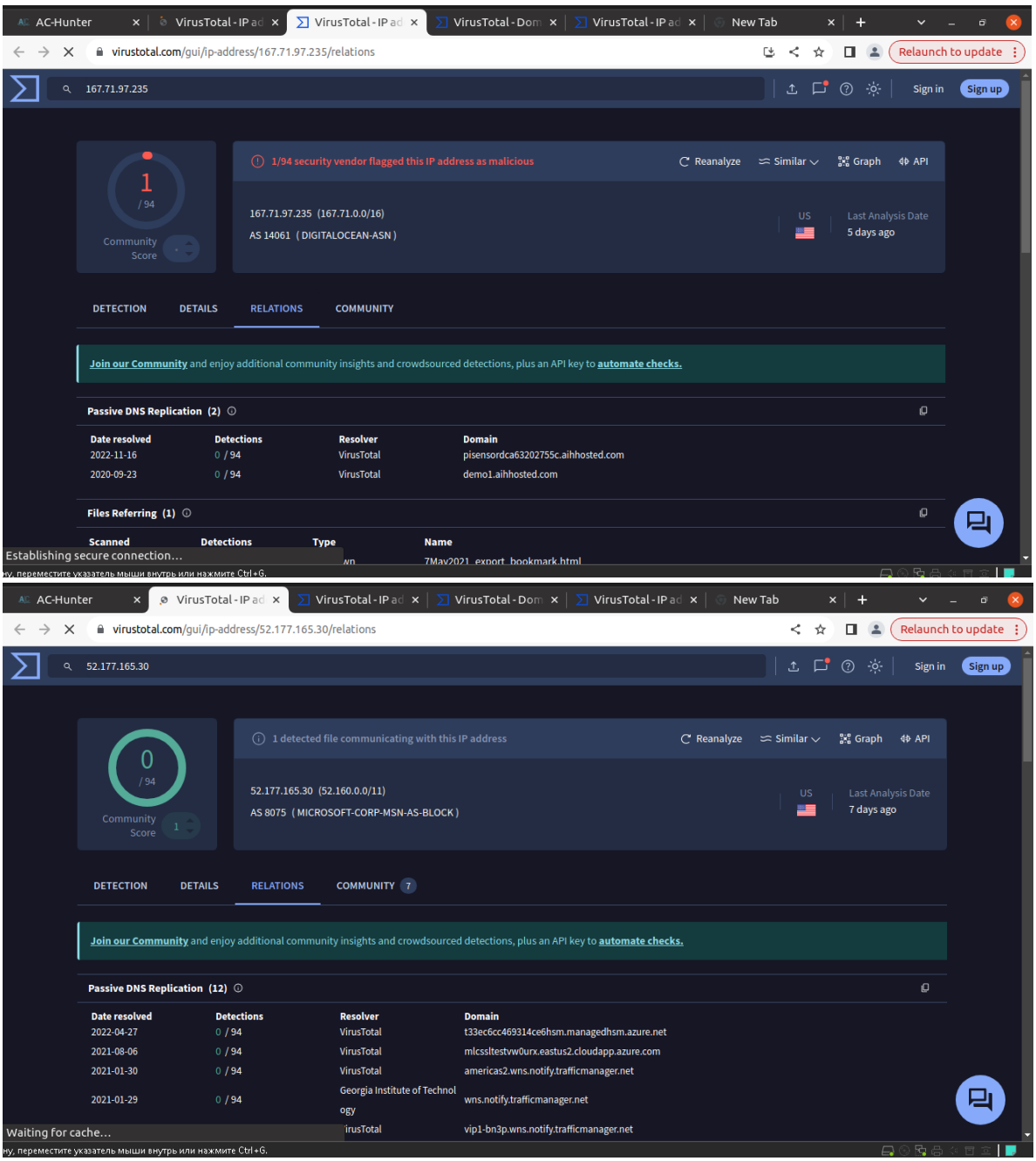
3) Видим запись с большим значение beacon. Домен хоть и похож на оригинальный скайп, но все-таки он отличается.

4) Так же как и первой части проверим через virustotal и видим что данный домен помечен как ненадёжный



5) Переходим во вкладку длительные подключения и видим такую же ситуацию, как и в первом наборе данных


AC-Hunter
VirusTotal - Domain - new
VirusTotal - IP address - 1
New Tab
Not secure | https://127.0.0.1/longconns/view1
Relaunch to update
SORT BY
Duration [▾]
DURATION THRESHOLD
5 hrs
SEARCH
SRC 192.168.99.54
[Private Network Address]
network name Unknown Private
DST 167.71.97.235
asn 14061
org DIGITALOCEAN-AS...
range 167.71.0.0/16
city Clifton, NJ
country United States
location 40.83841N, -74.1...
queried fqdn [no results]
historic fqdn [no results]
comm 9200:tcp:-
AC HUNTER
COMMUNITY EDITION
-- DATABASE: LAB3
-- MODULE: LONG CONNECTIONS
-- VIEW 1: TOTAL DURATION ANALYSIS
-- RANGE: 08/26/20 16:17 -- 09/27/20 16:17
Src
Src Network Name
Dst
Dst Network Name
Port:Protocol:Service
State
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
52.177.165.30
Public
443:tcp:ssl, 443:tcp:-
closed
494.94 kB
19:48:02
views
1 / 1
dashboard
beacons
beacons web
beacons proxy
strobes
long connections
threat intel
dns
client signature
cyber deception
deep dive
logout
ватель мыши наружу или нажмите Ctrl+Alt.



Вывод: делаем заключение что данный адрес является вредоносным