BeezPCAP Analysis Report

File: test

Timestamp: 20250511_195618



AI summary generation is disabled.

Enriched IOCs

45.125.66.252 | VT: Malicious | ISP: HostBaltic Lithuania | Country: LT | Usage: Data Center/Web Hosting/Transit

45.125.66.32 | VT: Malicious | AbuseIPDB Score: 82 | ISP: HostBaltic Lithuania | Country: LT | Usage: Data Center/Web Hosting/ Transit

5.252.153.241 | VT: Malicious | ISP: Partner Hosting LTD | Country: DE | Usage: Data Center/Web Hosting/Transit

185.188.32.26 | VT: Clean | ISP: TeamViewer Germany GmbH | Country: DE | Usage: Commercial

199.232.214.172 | VT: Clean | ISP: Fastly, Inc. | Country: US | Usage: Content Delivery Network

23.205.110.59 | VT: Clean | ISP: Akamai Technologies, Inc. | Country: US | Usage: Data Center/Web Hosting/Transit

23.220.102.9 | VT: Clean | ISP: Akamai Technologies, Inc. | Country: US | Usage: Data Center/Web Hosting/Transit

Suricata Alerts

 \bigcirc 2025-01-22T19:45:01.461001+0000 | 10.1.17.215 → 23.220.102.9 | *TCP* | ET INFO Microsoft Connection Test

 \triangle 2025-01-22T19:45:58.839654+0000 | 10.1.17.215 \rightarrow 5.252.153.241 | *TCP* | ET MALWARE Fake Microsoft Teams CnC Payload Request (GET)

 \triangle 2025-01-22T19:45:56.994934+0000 | 10.1.17.215 \rightarrow 5.252.153.241 | *TCP* | ET MALWARE Fake Microsoft Teams CnC Payload Request (GET)

<u>(a)</u> **2025-01-22T19:47:01.683653+0000** | 5.252.153.241 → 10.1.17.215 | *TCP* | ET HUNTING Generic Powershell DownloadString Command

<u>(a)</u> 2025-01-22T19:55:02.375410+0000 | 10.1.17.215 → 23.205.110.59 | *TCP* | ET INFO Microsoft Connection Test

 \bigcirc 2025-01-22T19:47:02.003020+0000 | 5.252.153.241 → 10.1.17.215 | *TCP* | ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download

<u> 2025-01-22T19:47:02.003020+0000</u> | 5.252.153.241 → 10.1.17.215 | *TCP* | ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response

 \bigcirc 2025-01-22T19:59:46.284354+0000 | 45.125.66.32 → 10.1.17.215 | *TCP* | ET DROP Spamhaus DROP Listed Traffic Inbound group 4

 \triangle 2025-01-22T19:47:05.679743+0000 | 10.1.17.215 → 5.252.153.241 | *TCP* | ET INFO PS1 Powershell File Request

2025-01-22T20:04:24.443346+0000 | 199.232.214.172 → 10.1.17.215 | *TCP* | ET INFO Packed Executable Download

<u>(a)</u> 2025-01-22T19:44:56.530137+0000 | 5.252.153.241 → 10.1.17.215 | *TCP* | ET MALWARE Fake Microsoft Teams VBS Payload Inbound

 \bigcirc 2025-01-22T19:44:56.530137+0000 | 5.252.153.241 → 10.1.17.215 | *TCP* | ET ATTACK_RESPONSE PowerShell NoProfile Command Received In Powershell Stagers

DNS Queries

- 224.0.0.252
- **10.1.17.2**
- 224.0.0.251
- *>* 10.1.17.255

Zeek HTTP Requests

- 1GET | UA: /connecttest.txt
- 1GET | UA: /api/file/get-file/264872
- ### 1GET | UA: /api/file/get-file/29842.ps1
- (iii) 2GET | UA: /1517096937
- () 3GET | UA: /1517096937
- ### 4GET | UA: /1517096937

⊕ 5GET | UA: /1517096937

 ⊕ 6GET | UA: /1517096937

THEAD | UA: /filestreamingservice/files/2ed1297ef6c9-4355-aec4-433ea371b116?
P1=1737884967&P2=404&P3=2&P4=DQ/
rdpZetb6+CA7SUqm0gjEUa0b3x/0sl0Rjy3dXLFk/
x6KtXqpmjgm4wKw8TSyht7Eu00wi6QlvL9zKqBzIFw==

2GET | UA: /filestreamingservice/files/2ed1297ef6c9-4355-aec4-433ea371b116?
P1=1737884967&P2=404&P3=2&P4=DQ/
rdpZetb6+CA7SUqmOgjEUa0b3x/0slORjy3dXLFk/
x6KtXqpmjgm4wKw8TSyht7Eu00wi6QlvL9zKqBzIFw==

(7GET | UA: /1517096937

3HEAD | UA: /filestreamingservice/files/2a0d597ca09c-4400-be86-87596dd2e696?

P1=1737884967&P2=404&P3=2&P4=W7W0p0Z6ahXXhvqsFdcWAJHdZVPv8SRh1FficfbizEC

4GET | UA: /filestreamingservice/files/2a0d597c-a09c-4400-be86-87596dd2e696?

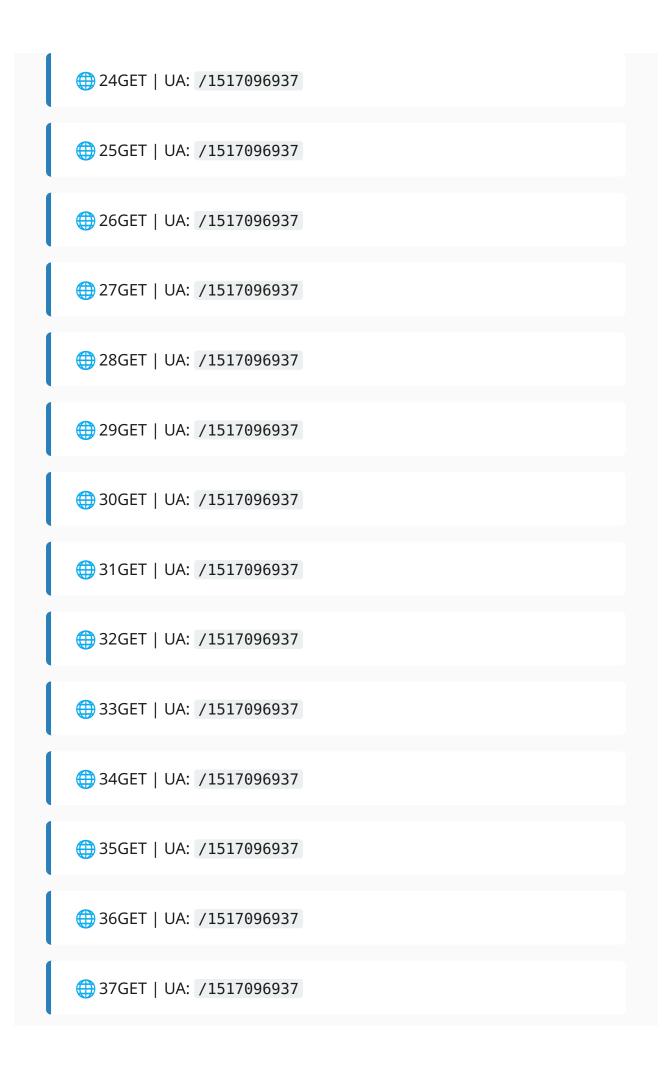
P1=1737884967&P2=404&P3=2&P4=W7W0p0Z6ahXXhvqsFdcWAJHdZVPv8SRh1FficfbizEC

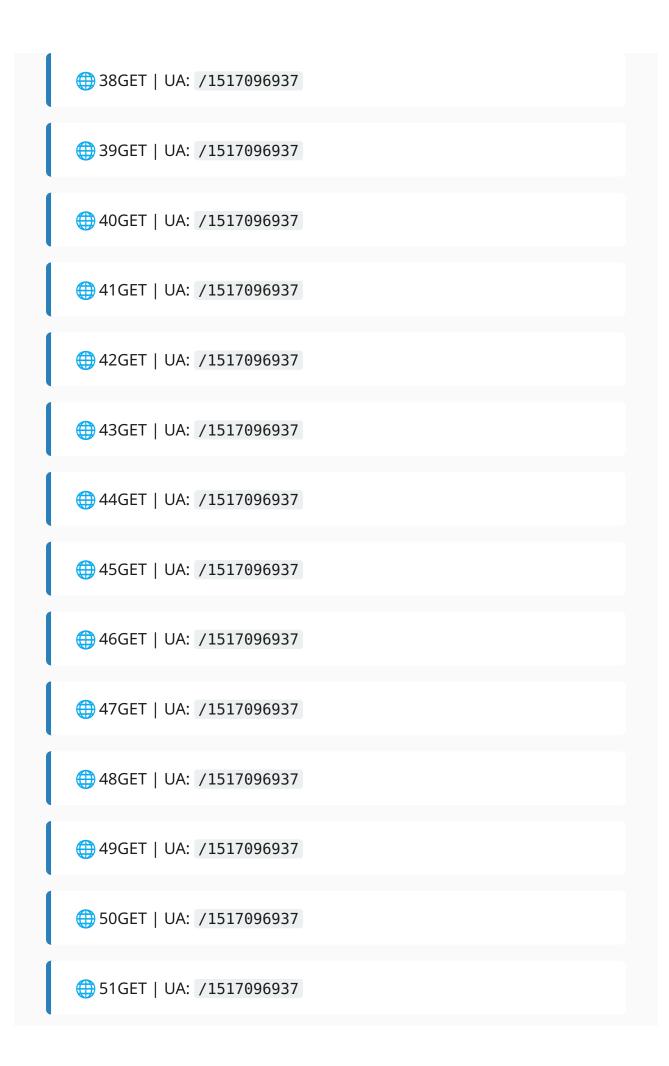
8GET | UA: /1517096937

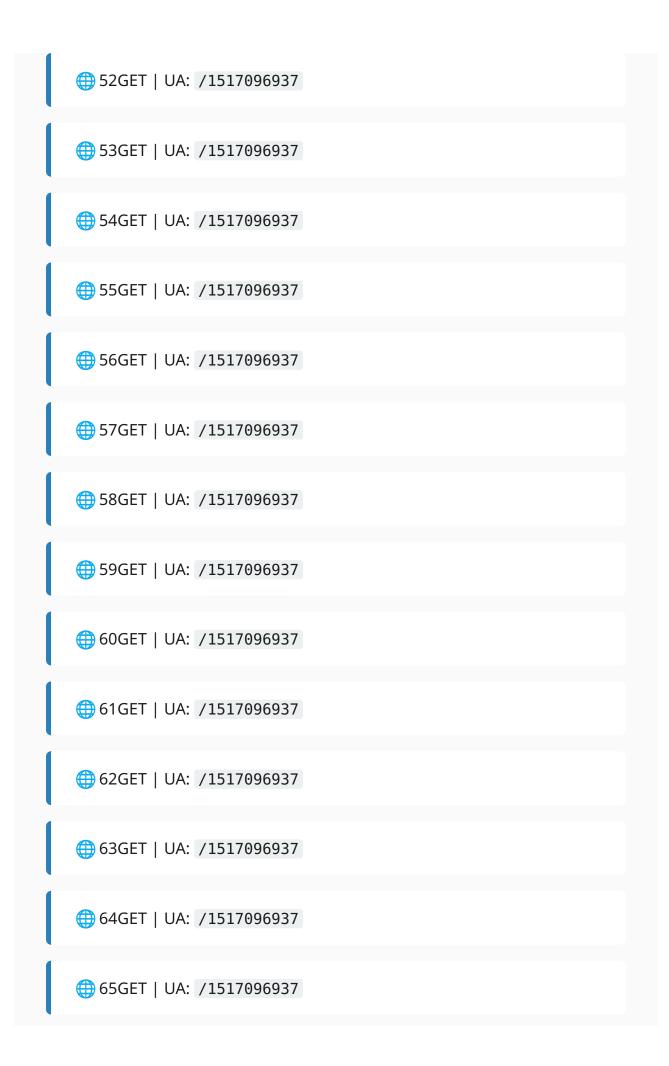
9GET | UA: /1517096937

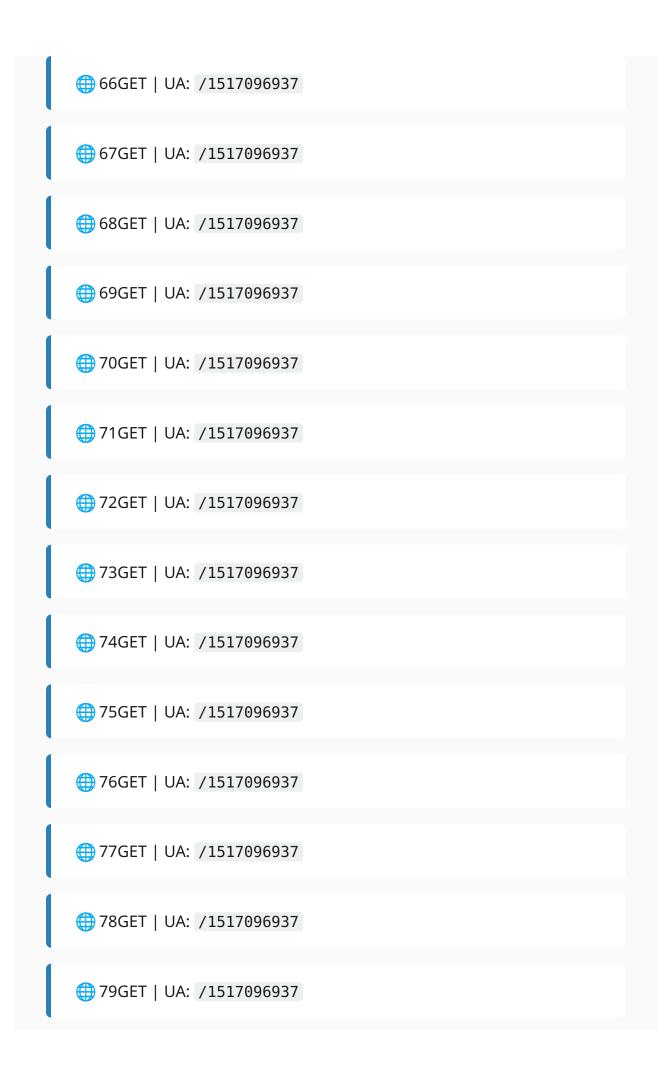
(10GET | UA: /1517096937

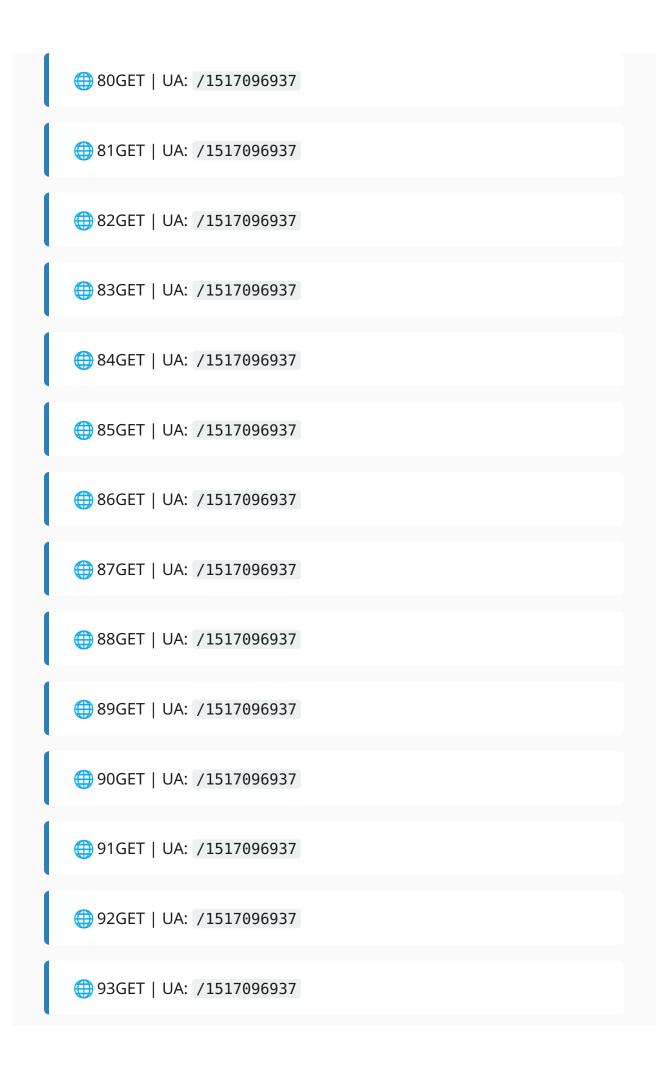
```
( 11GET | UA: /1517096937
( 12GET | UA: /1517096937
(iii) 13GET | UA: /1517096937
( 14GET | UA: /1517096937
15GET | UA: /api/file/get-file/TeamViewer
16GET | UA: /api/file/get-file/Teamviewer_Resource_fr
17GET | UA: /api/file/get-file/TV
18GET | UA: /api/file/get-file/pas.ps1
19GET | UA: /1517096937?k=message = startup shortcut
created; status = success;
( 20GET | UA: /1517096937
(m) 21GET | UA: /1517096937
( 22GET | UA: /1517096937
( 23GET | UA: /1517096937
```











```
(iii) 94GET | UA: /1517096937
1GET | UA: /connecttest.txt
(iii) 1GET | UA: /1517096937
(iii) 1GET | UA: /din.aspx?
s=00000000&id=0&client=DynGate&rnd=427975263&p=10000001
## 2GET | UA: /dout.aspx?
s=91930119&p=10000001&client=DynGate&data=FyQSkgCjHqkys5MkoZ6ZGhycGJuamZ
3GET | UA: /din.aspx?
s=91930119&id=0&client=DynGate&p=10000002
(iii) 1GET | UA: /din.aspx?
s=91930119&id=0&client=DynGate&p=10000002
1GET | UA: /din.aspx?
s=00000000&id=0&client=DynGate&rnd=15187500&p=10000001
## 2GET | UA: /dout.aspx?
s=91930135&p=10000001&client=DynGate&data=FyQSkgCjHqkys5MkoZ6ZGhycGJuamZ
3GET | UA: /din.aspx?
s=91930135&id=0&client=DynGate&p=10000002
1GET | UA: /din.aspx?
s=91930135&id=0&client=DynGate&p=10000002
```

```
    1GET | UA: /din.aspx?
s=00000000&id=0&client=DynGate&rnd=216758732&p=10000001
```

GET | UA: /dout.aspx?
s=91930144&p=10000001&client=DynGate&data=FyQSkgCjHqkys5MkoZ6ZGhycGJuamZ

3GET | UA: /din.aspx?
s=91930144&id=0&client=DynGate&p=10000002

1GET | UA: /din.aspx?
s=91930144&id=0&client=DynGate&p=10000002

1GET | UA: /din.aspx?
s=00000000&id=0&client=DynGate&rnd=418412399&p=10000001

2GET | UA: /dout.aspx?
s=91930165&p=10000001&client=DynGate&data=FyQSkgCjHqkys5MkoZ6ZGhycGJuamZ

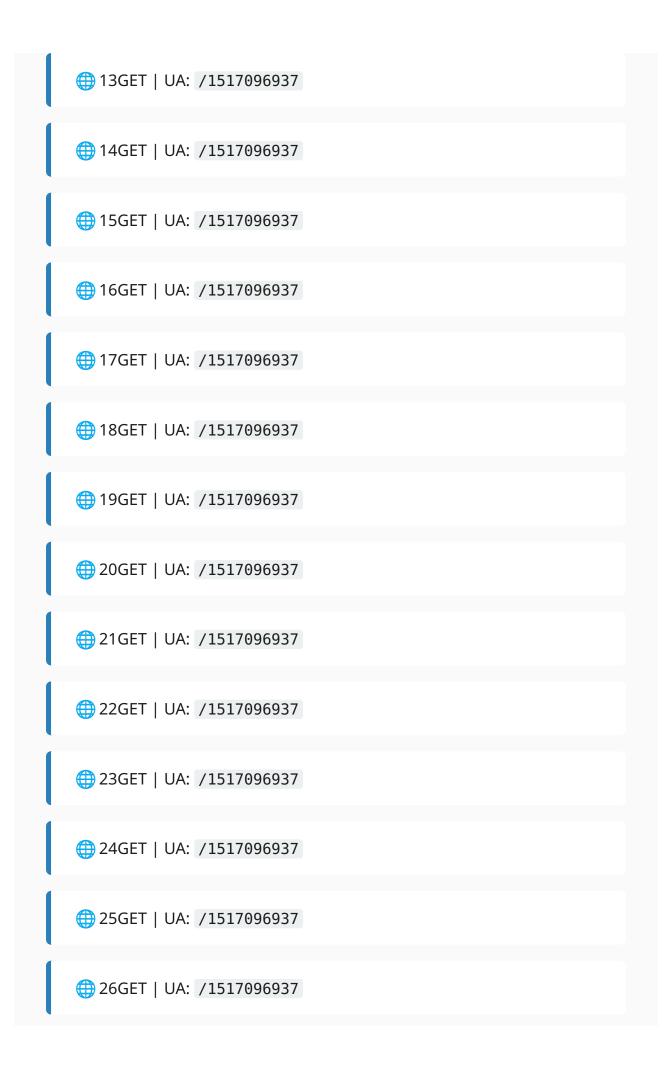
3GET | UA: /din.aspx?
s=91930165&id=0&client=DynGate&p=10000002

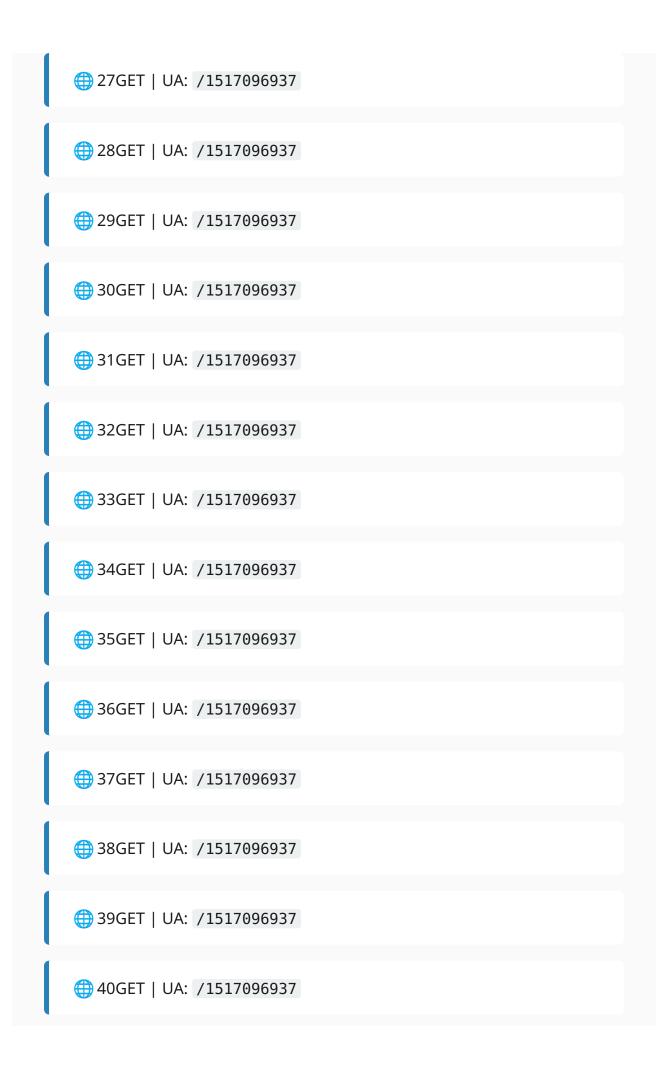
1GET | UA: /din.aspx?
s=91930165&id=0&client=DynGate&p=10000002

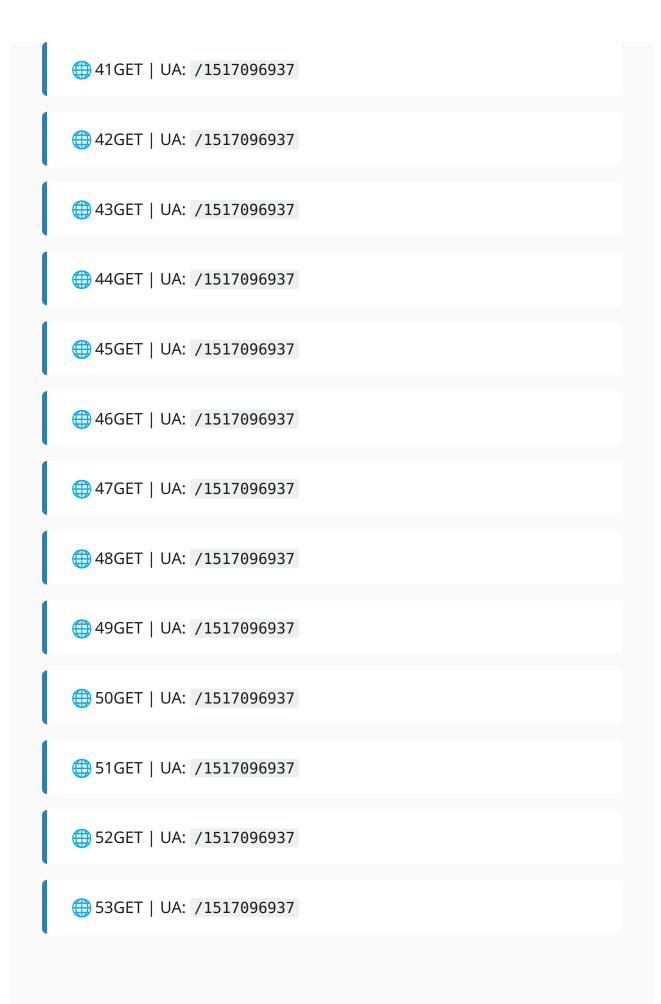
1GET | UA: /din.aspx?
s=00000000&id=0&client=DynGate&rnd=5384120&p=10000001

2GET | UA: /dout.aspx?
s=91930189&p=10000001&client=DynGate&data=FyQSkgCjHqkys5MkoZ6ZGhycGJuamZ

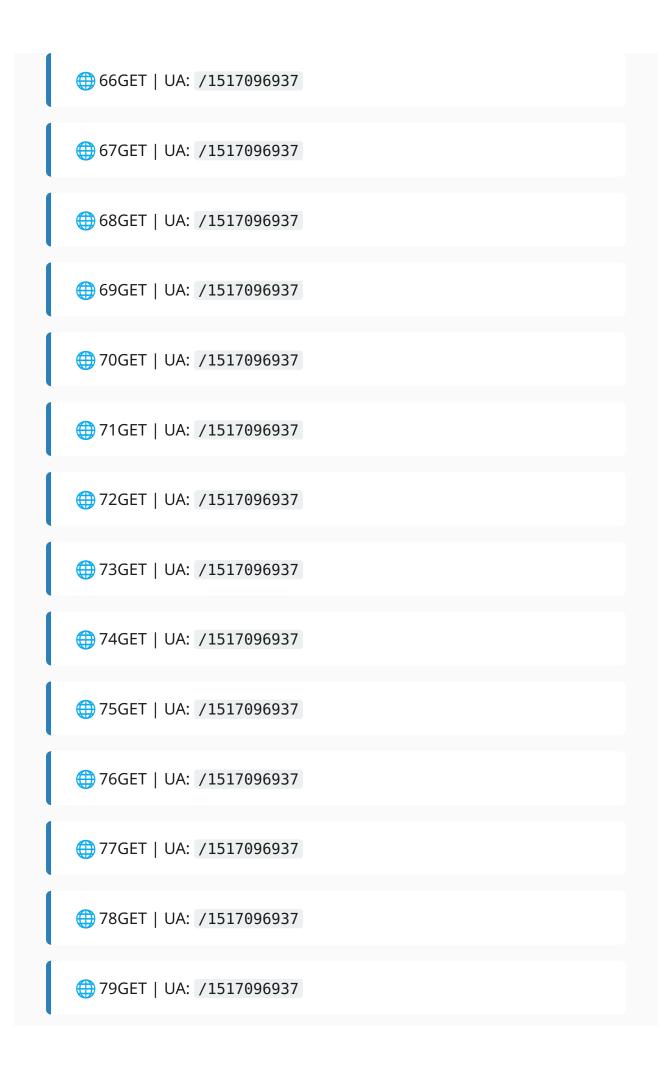
```
3GET | UA: /din.aspx?
s=91930189&id=0&client=DynGate&p=10000002
s=91930189&id=0&client=DynGate&p=10000002
( ) 2GET | UA: /1517096937
( ) 3GET | UA: /1517096937
### 4GET | UA: /1517096937
⊕ 5GET | UA: /1517096937
⊕ 6GET | UA: /1517096937
( 7GET | UA: /1517096937
⊕ 8GET | UA: /1517096937
( ) 9GET | UA: /1517096937
( 10GET | UA: /1517096937
( 11GET | UA: /1517096937
(m) 12GET | UA: /1517096937
```

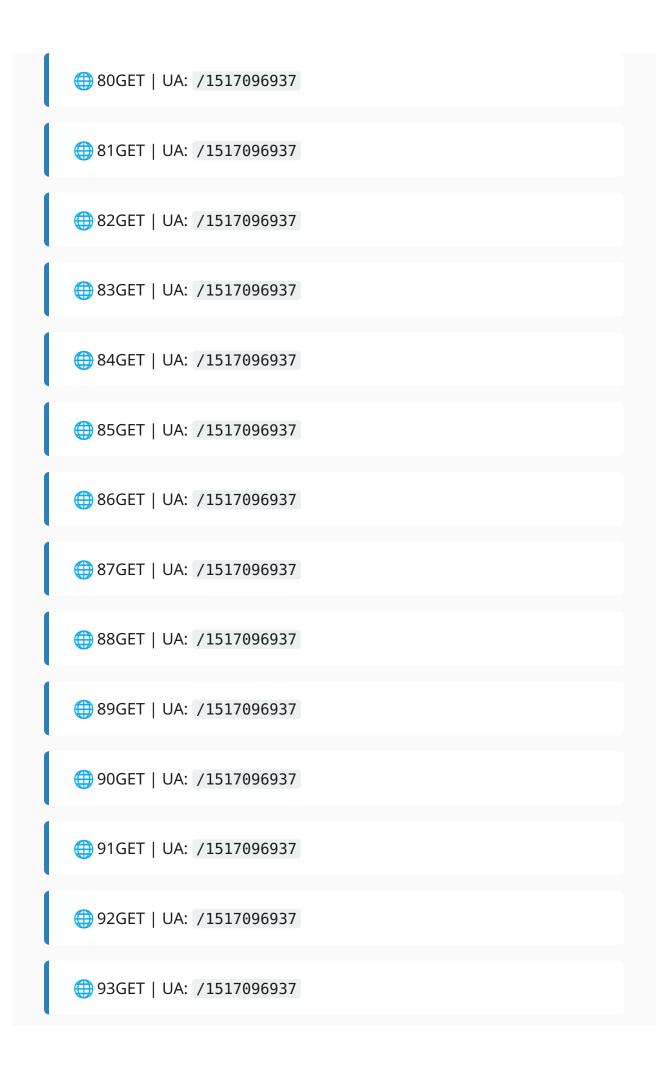


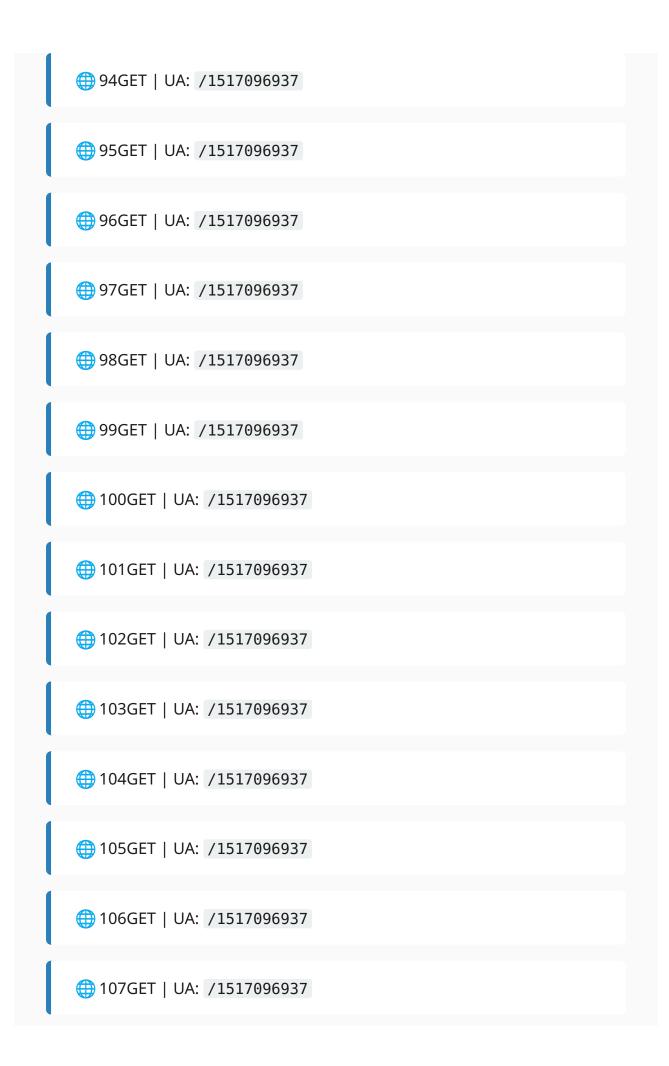




⇒ 54GET | UA: /1517096937?k=script: RunRH, status: OK, message: PS process started ⊕ 55GET | UA: /1517096937 ⊕ 56GET | UA: /1517096937 ⊕ 57GET | UA: /1517096937 ⊕ 58GET | UA: /1517096937 ⊕ 59GET | UA: /1517096937 s=91930119&id=0&client=DynGate&p=10000002 ⊕ 60GET | UA: /1517096937 (61GET | UA: /1517096937 (62GET | UA: /1517096937 (63GET | UA: /1517096937 ⊕ 64GET | UA: /1517096937 (65GET | UA: /1517096937



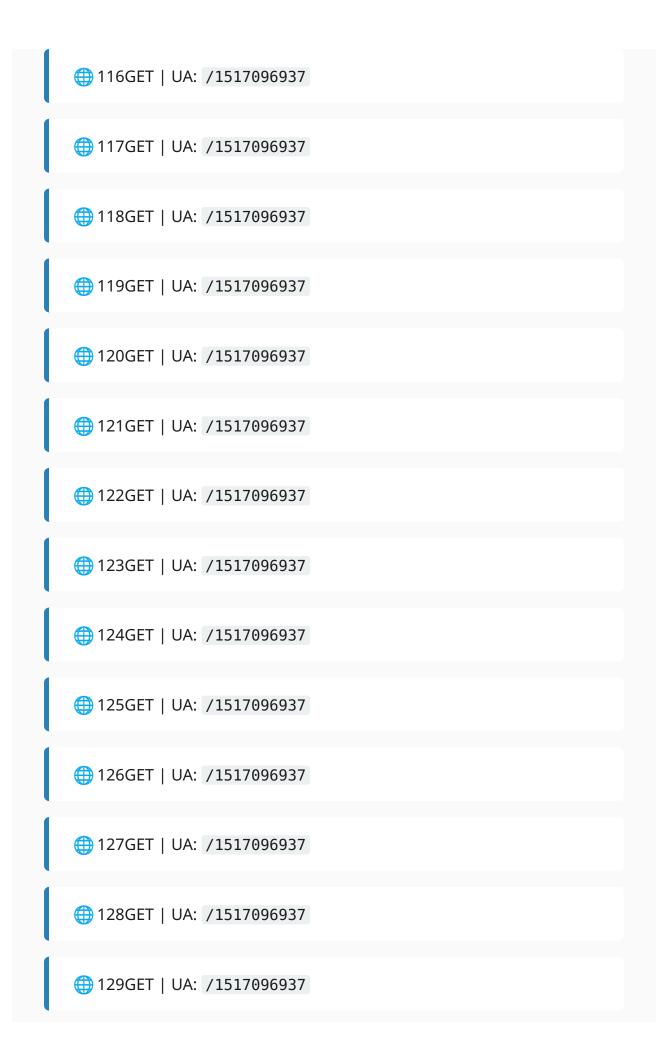


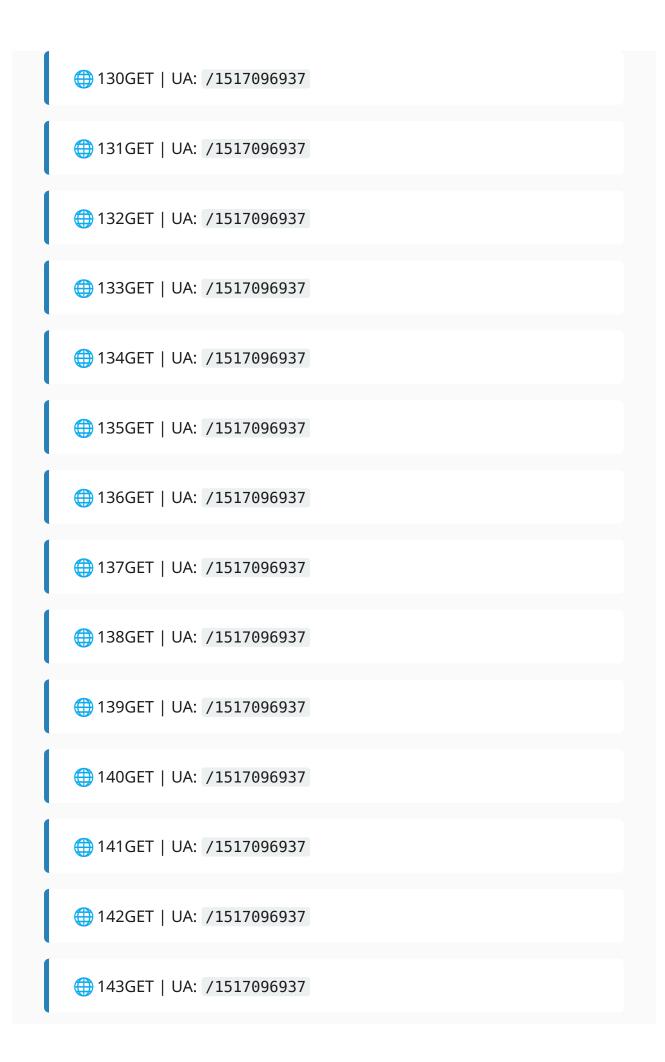


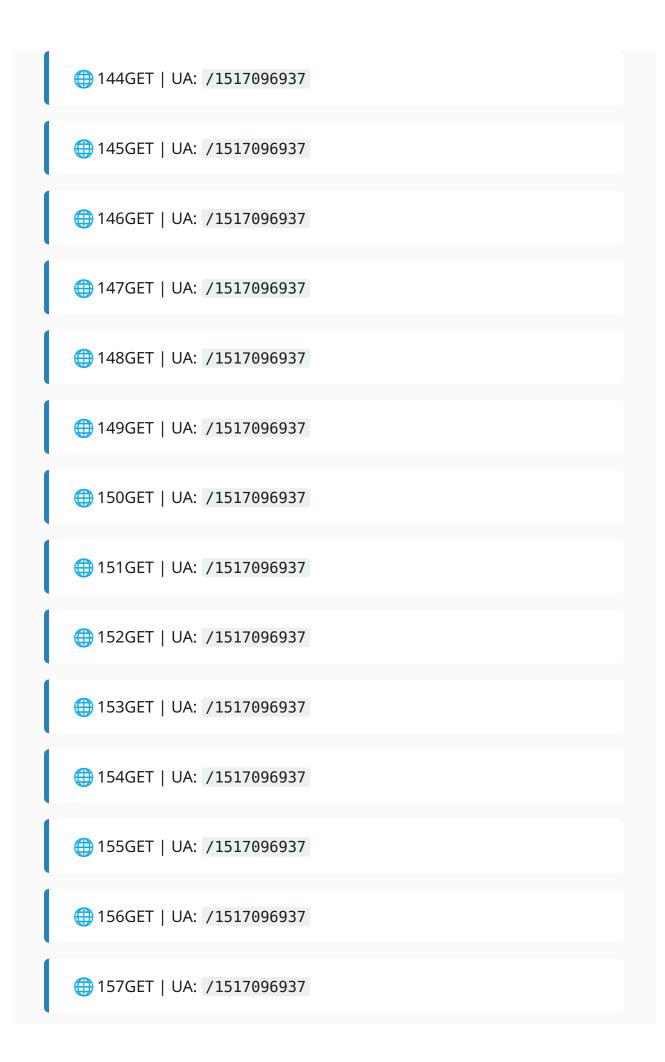
```
(iii) 108GET | UA: /1517096937
1GET | UA: /c/msdownload/update/others/
2025/01/42681409 9e243120ff356d59920855fa02c873fcbcf678c6.cab

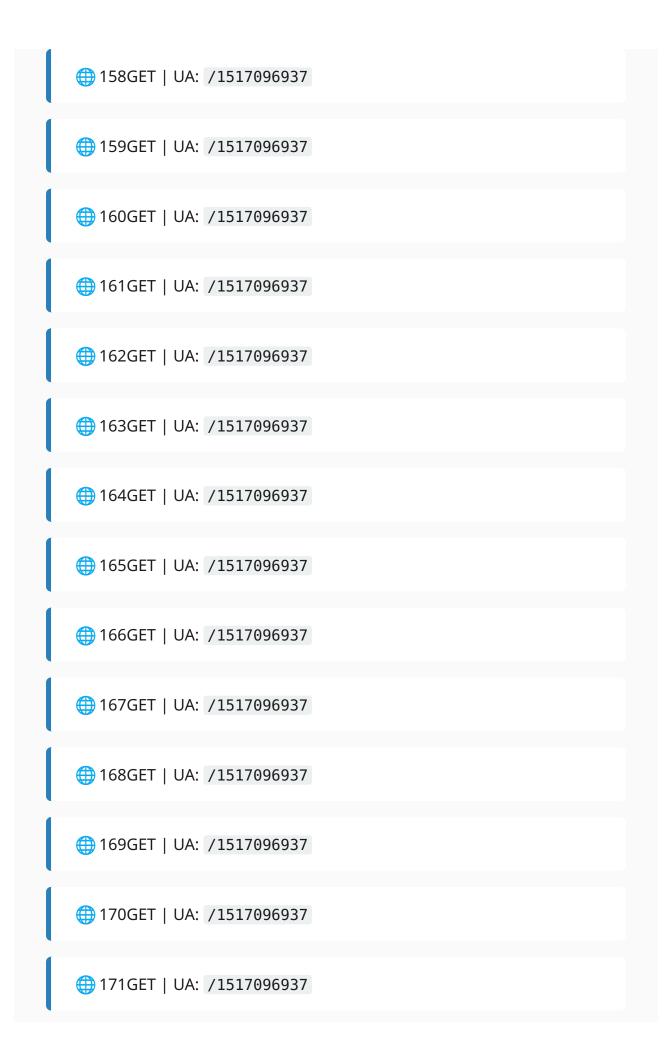
② 2GET | UA: /c/msdownload/update/others/

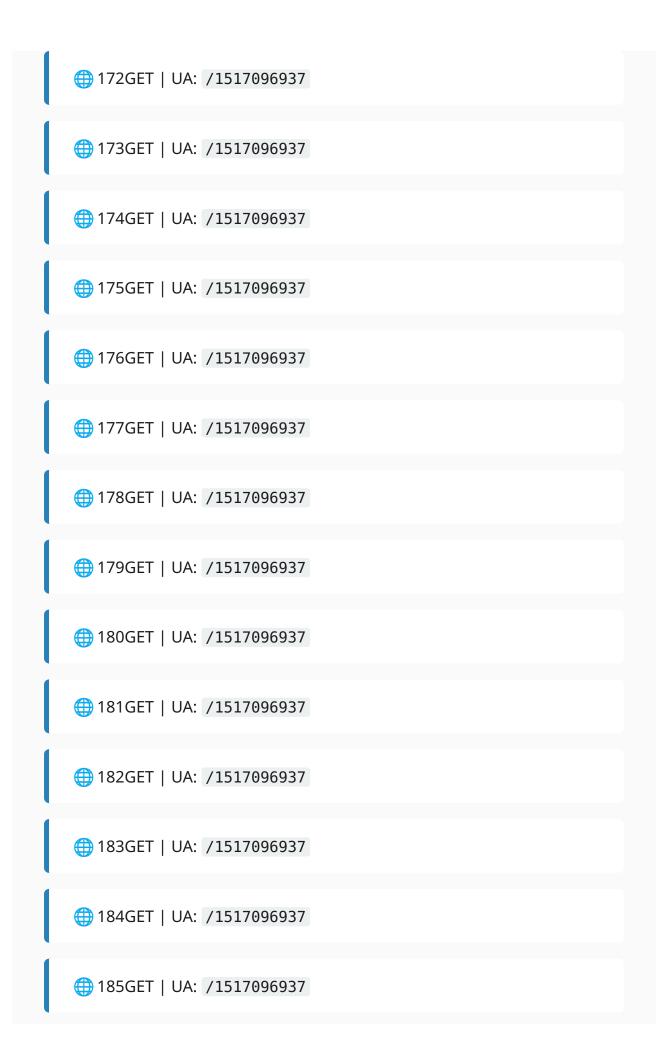
2025/01/42681408 eba72ad8cac00ea04690b09c0ff175074bb281e9.cab
3GET | UA: /c/msdownload/update/others/
2025/01/42681502 106431d428d2c49b06bf00d7ab662ff53edb4726.cab
1GET | UA: /c/msdownload/update/software/defu/2025/01/
am delta patch 1.421.1491.0 c8e6042b36d8f357a8e298b6f9f2fcde561c2e02.exe
(iii) 109GET | UA: /1517096937
(iii) 110GET | UA: /1517096937
(math) 111GET | UA: /1517096937
( 112GET | UA: /1517096937
( 113GET | UA: /1517096937
( 114GET | UA: /1517096937
( 115GET | UA: /1517096937
```

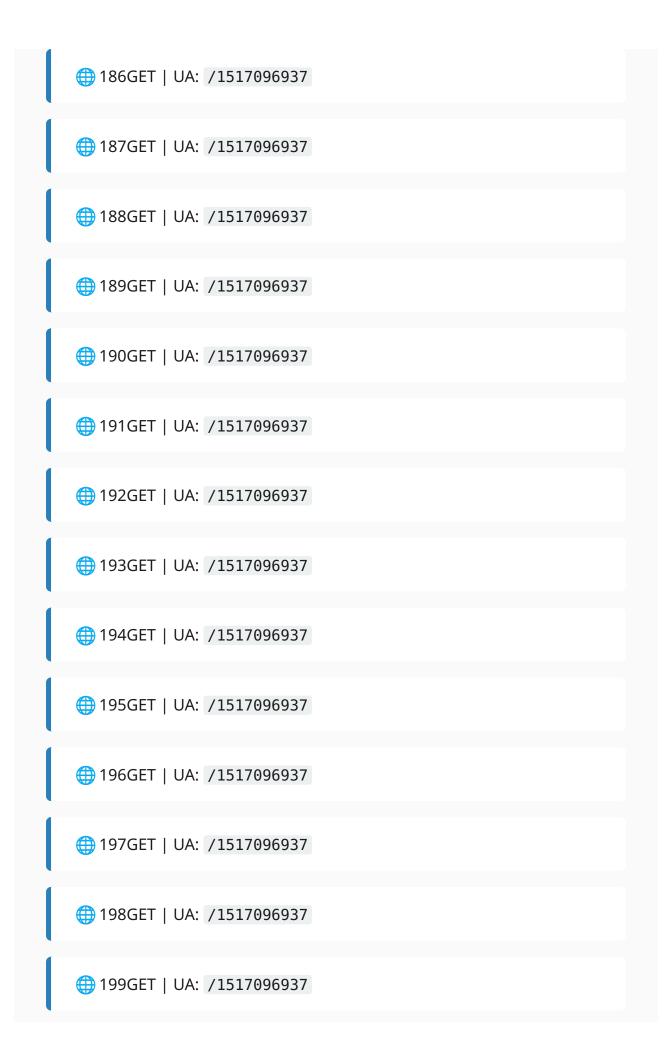


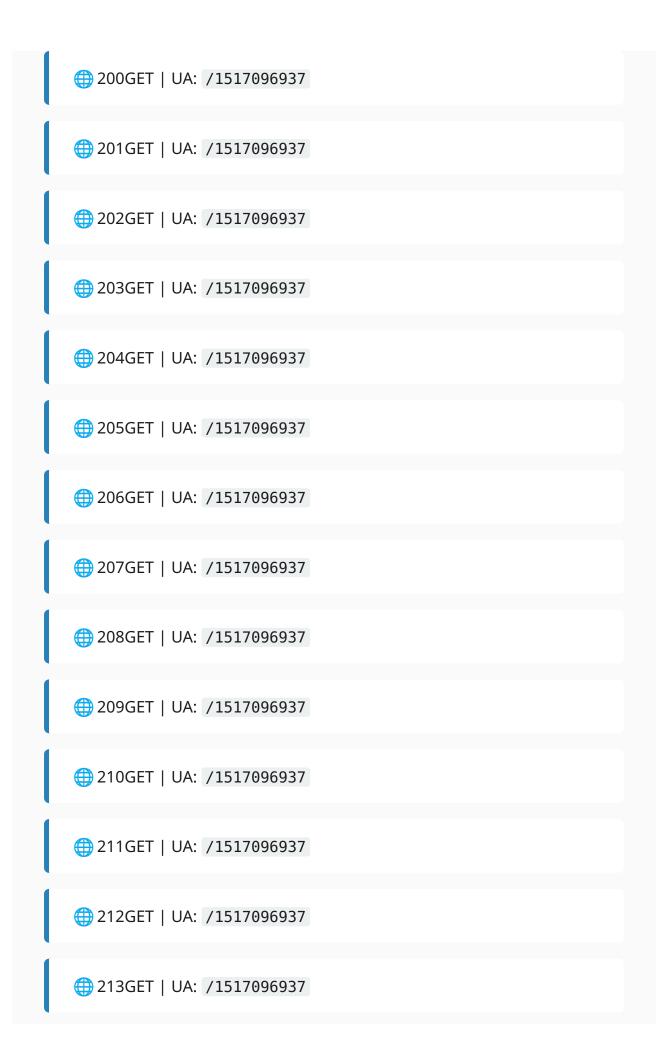


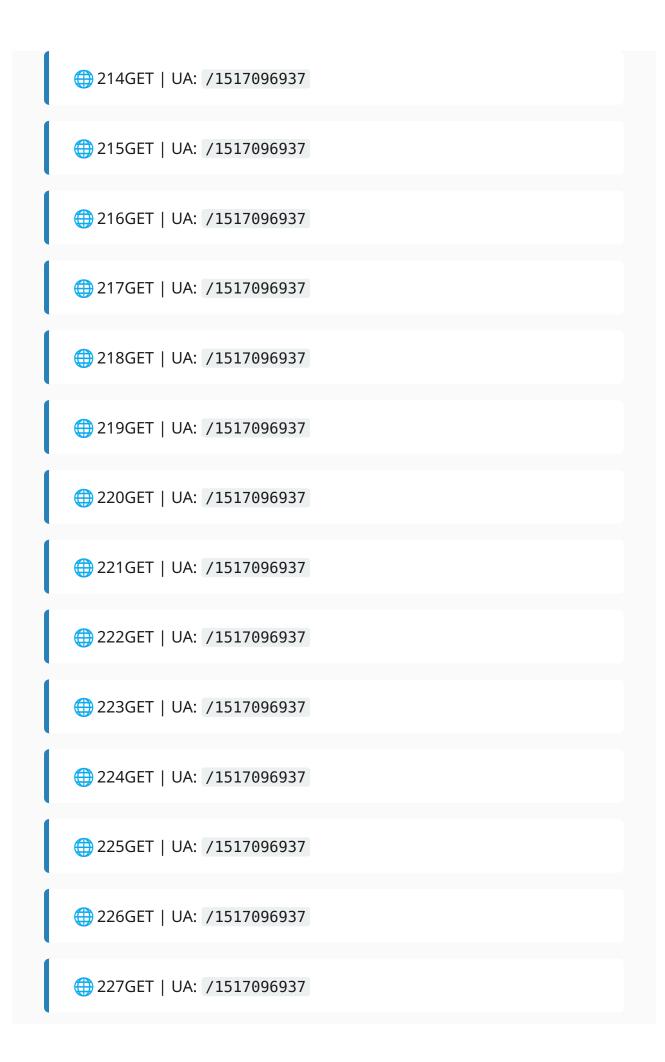


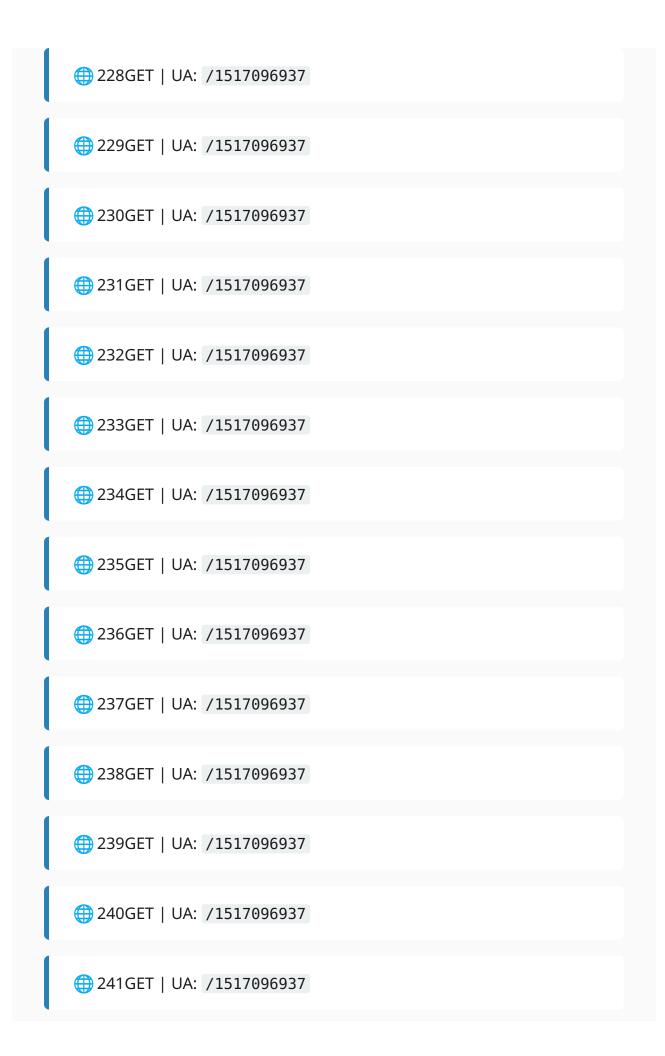


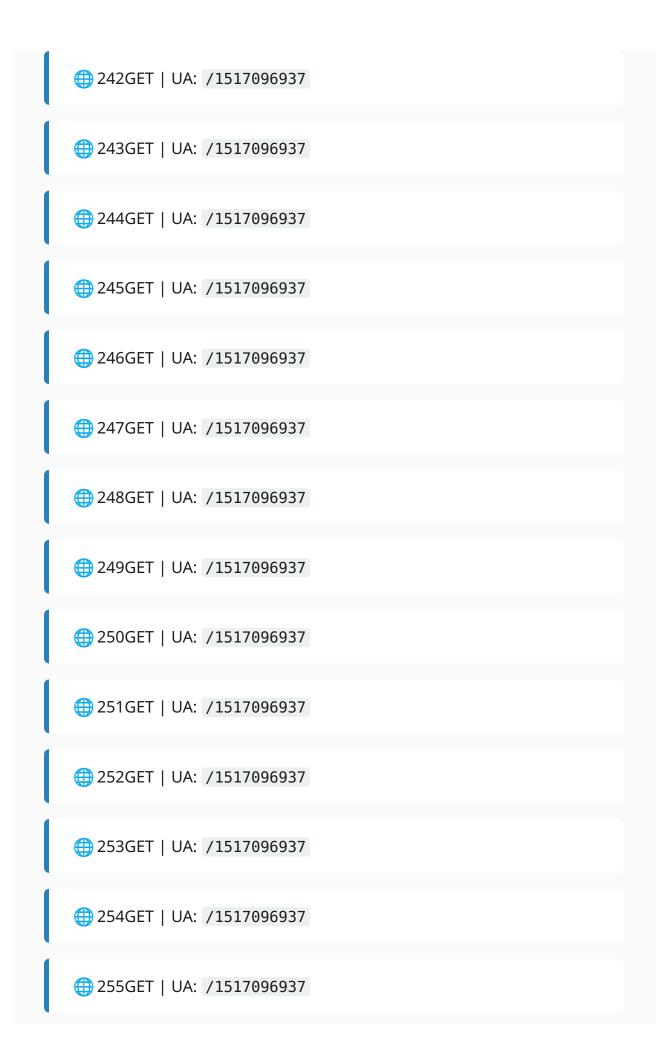


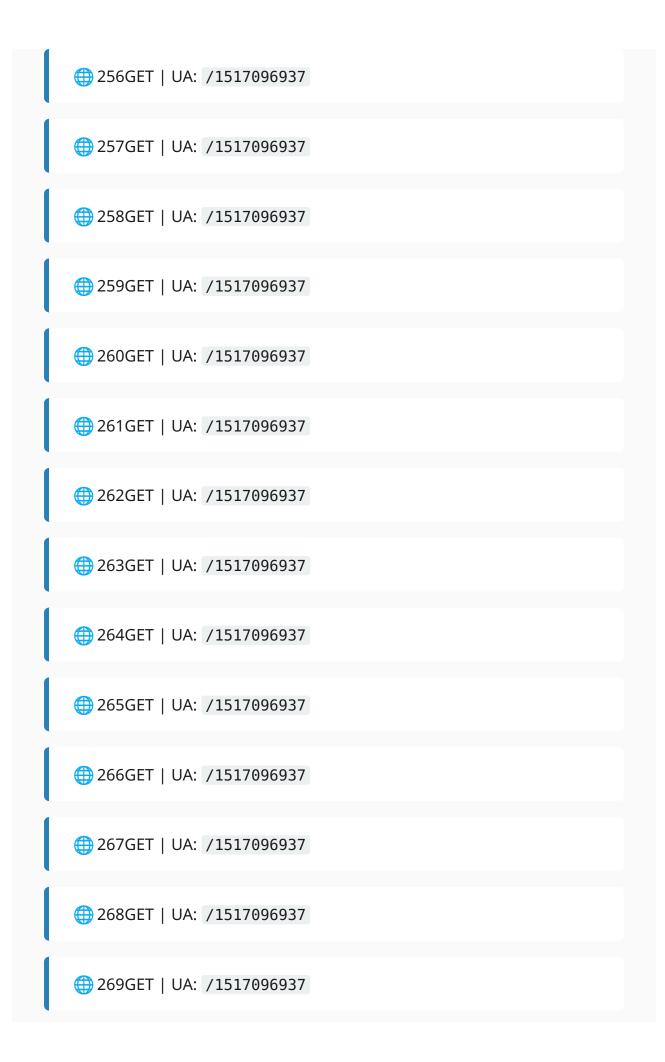


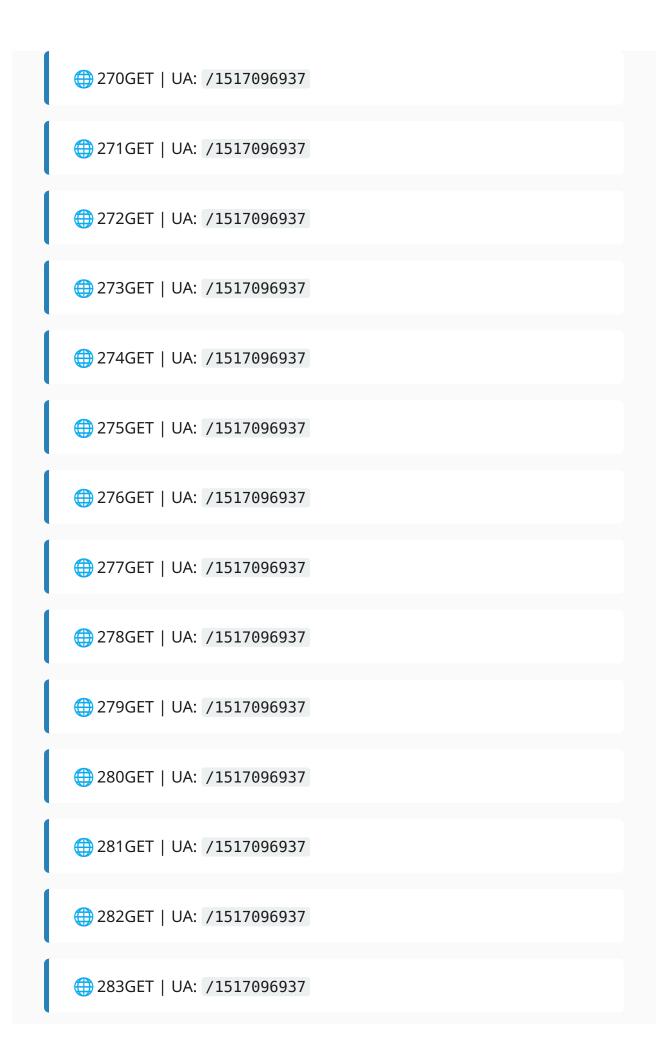


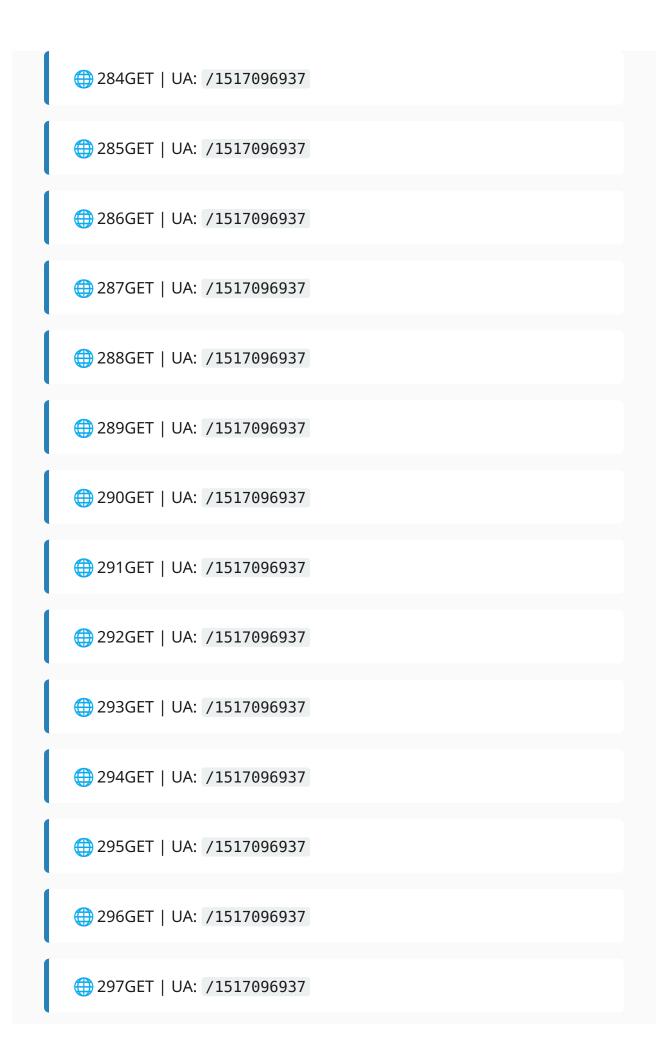


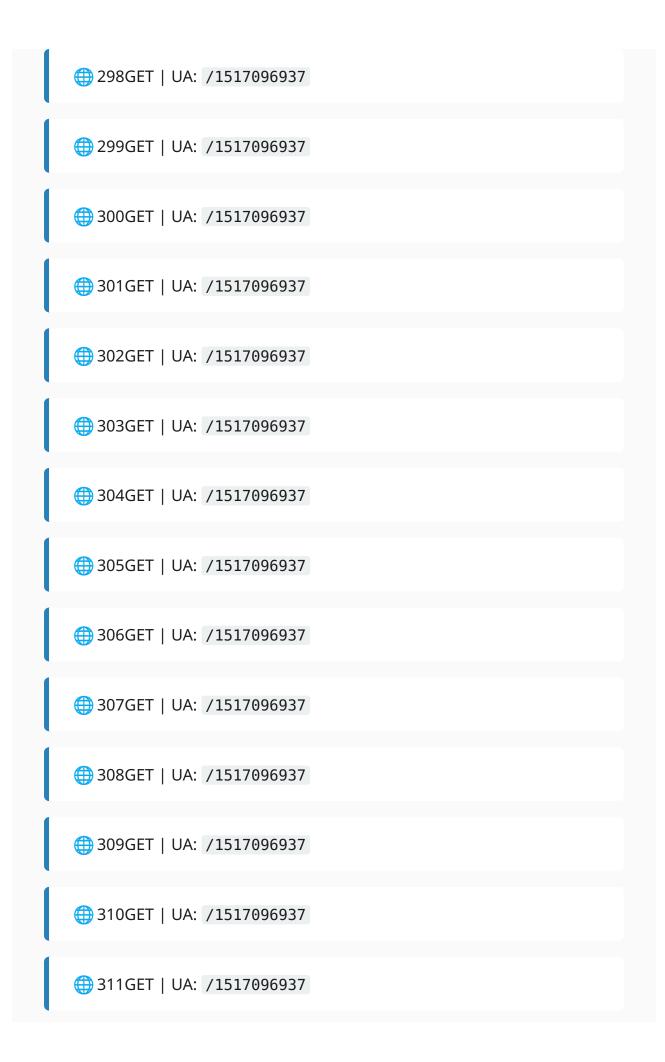


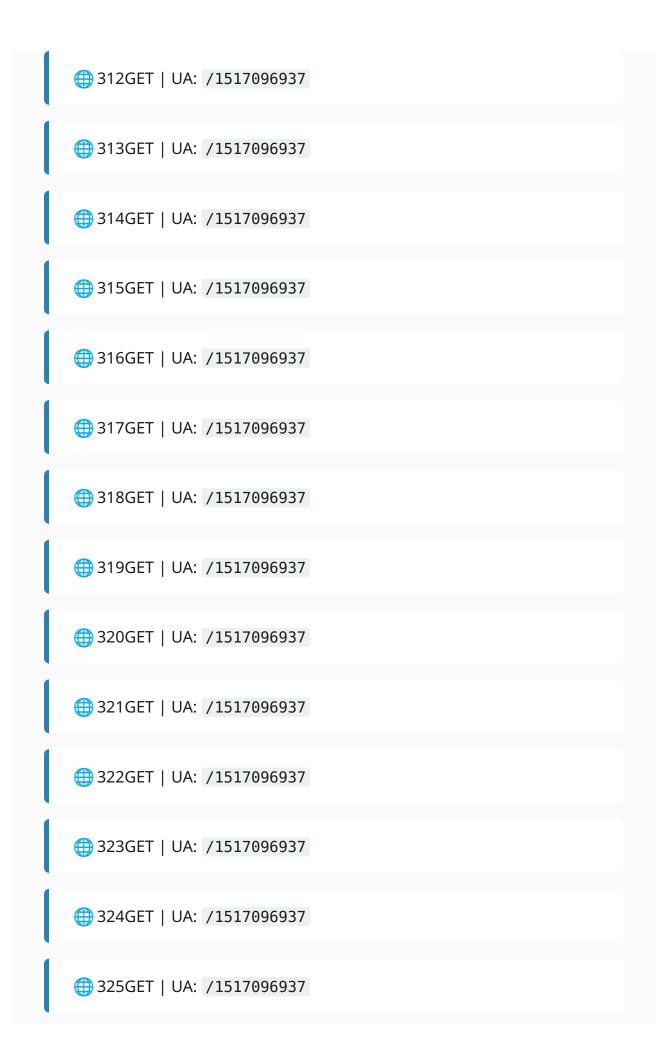


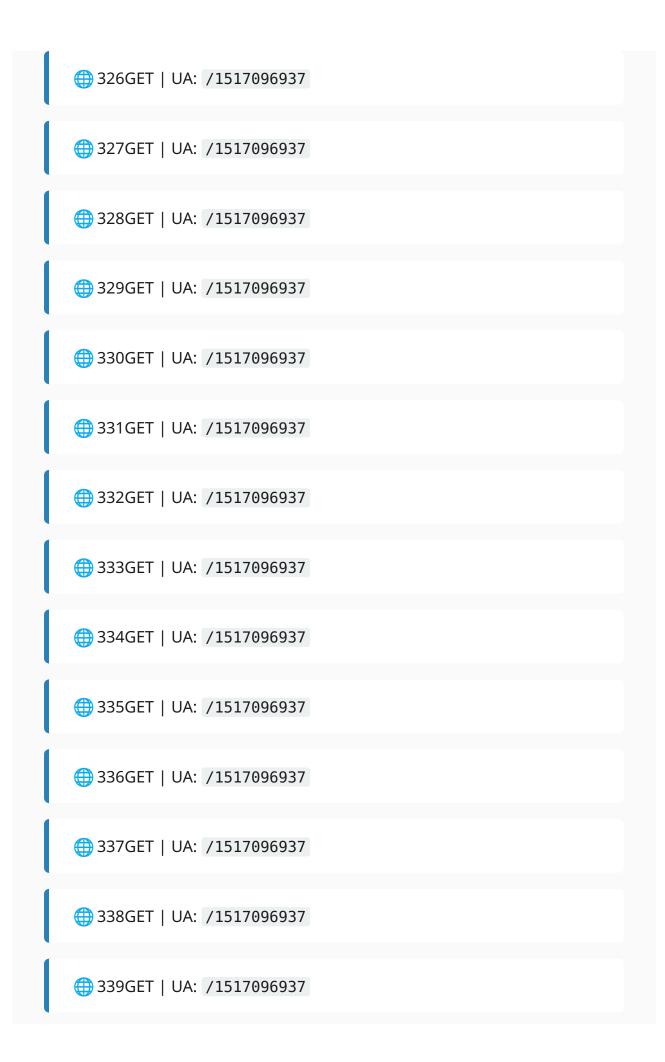




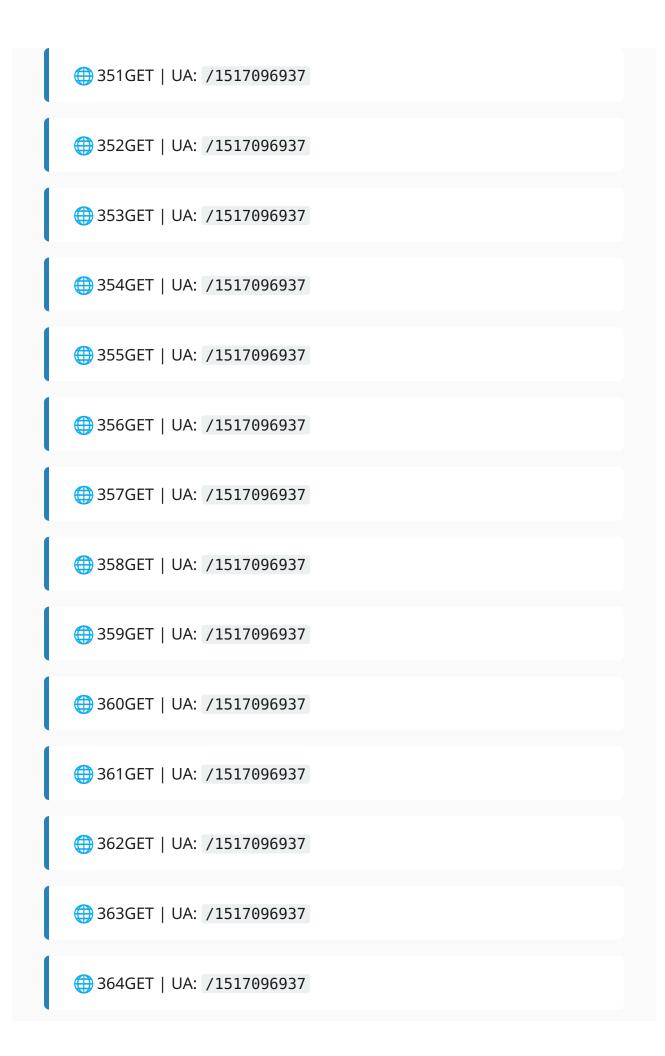


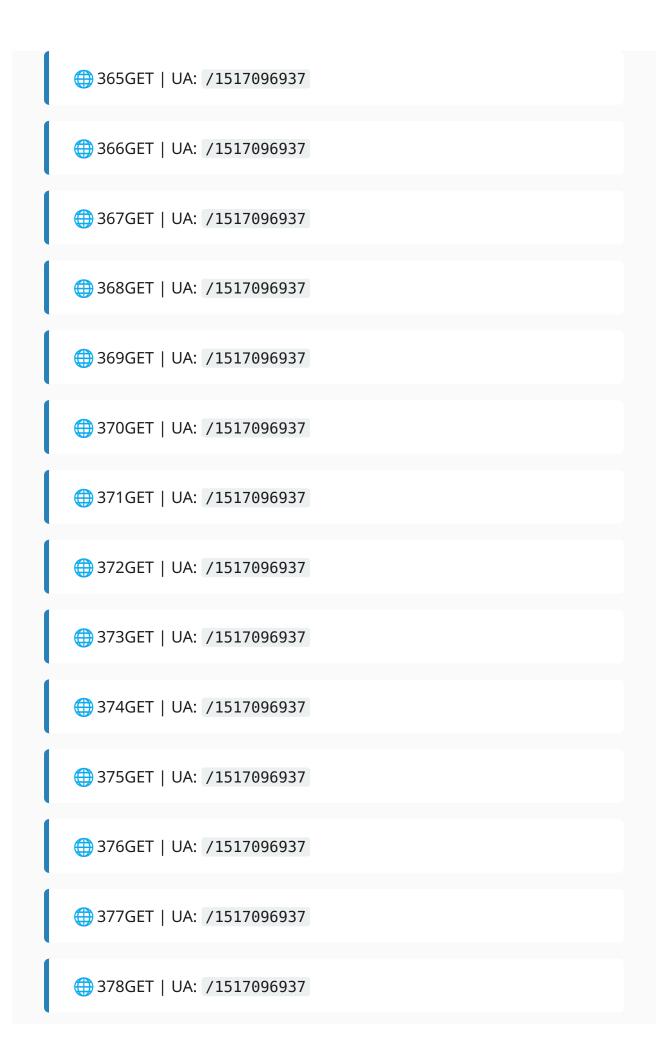




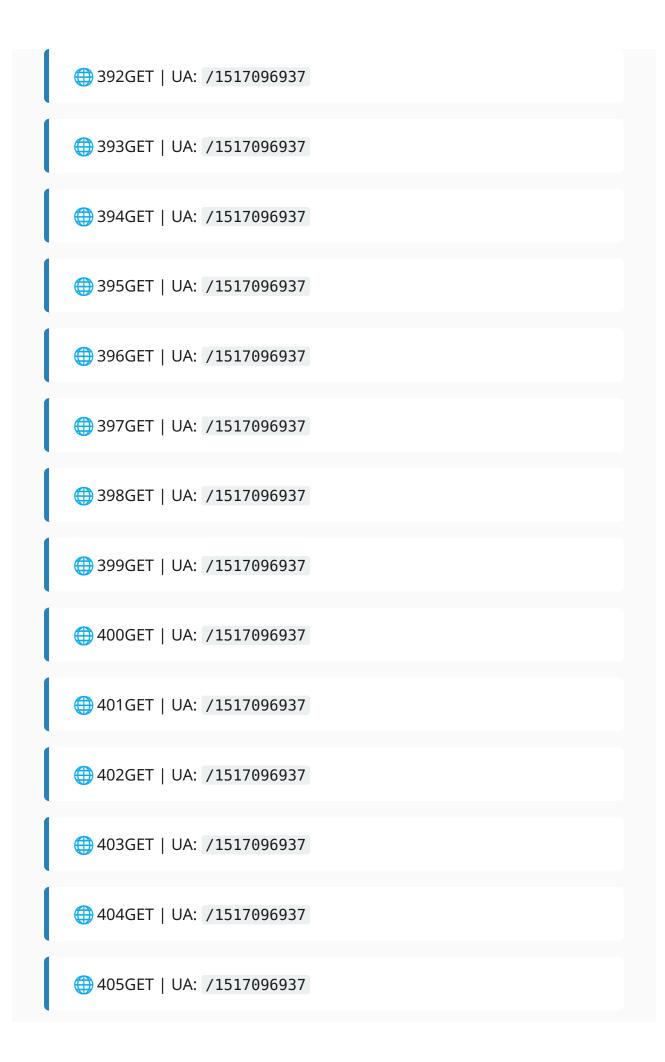


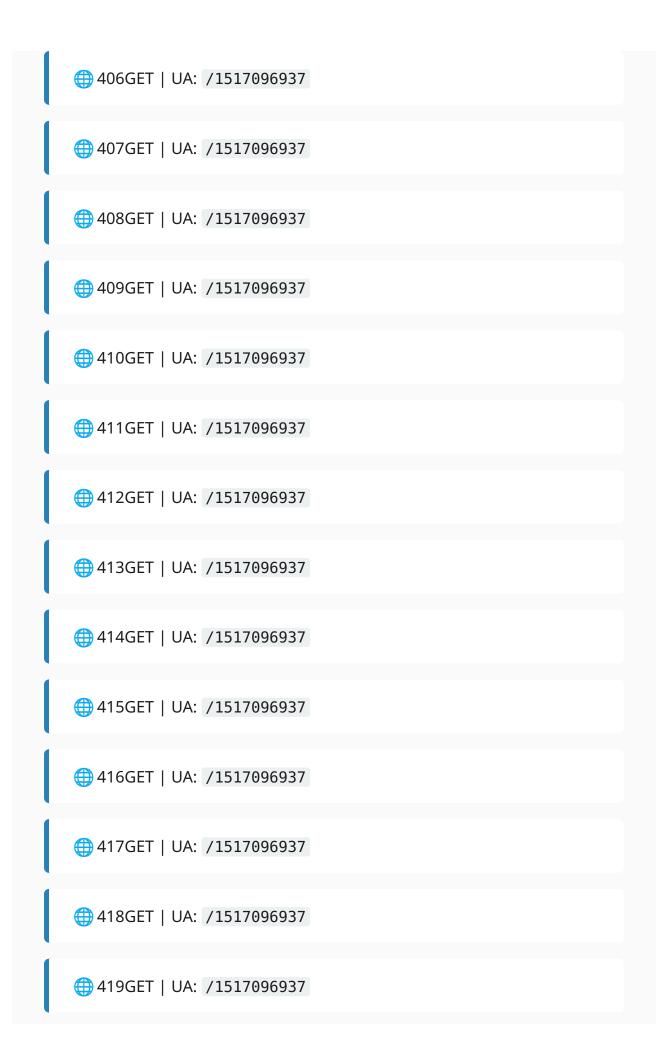
```
(iii) 340GET | UA: /1517096937
( 341GET | UA: /1517096937
(m) 342GET | UA: /1517096937
(m) 343GET | UA: /1517096937
(iii) 344GET | UA: /1517096937
(iii) 345GET | UA: /1517096937
( 346GET | UA: /1517096937
1GET | UA: /msdownload/update/v3/static/trustedr/en/
disallowedcertstl.cab?4dffb45145e1134f
## 2GET | UA: /msdownload/update/v3/static/trustedr/en/
pinrulesstl.cab?4f7e71b5ae12458e
( 347GET | UA: /1517096937
348GET | UA: /1517096937?k=script: RunRH, status: OK,
message: PS process started
( 349GET | UA: /1517096937
( 350GET | UA: /1517096937
```

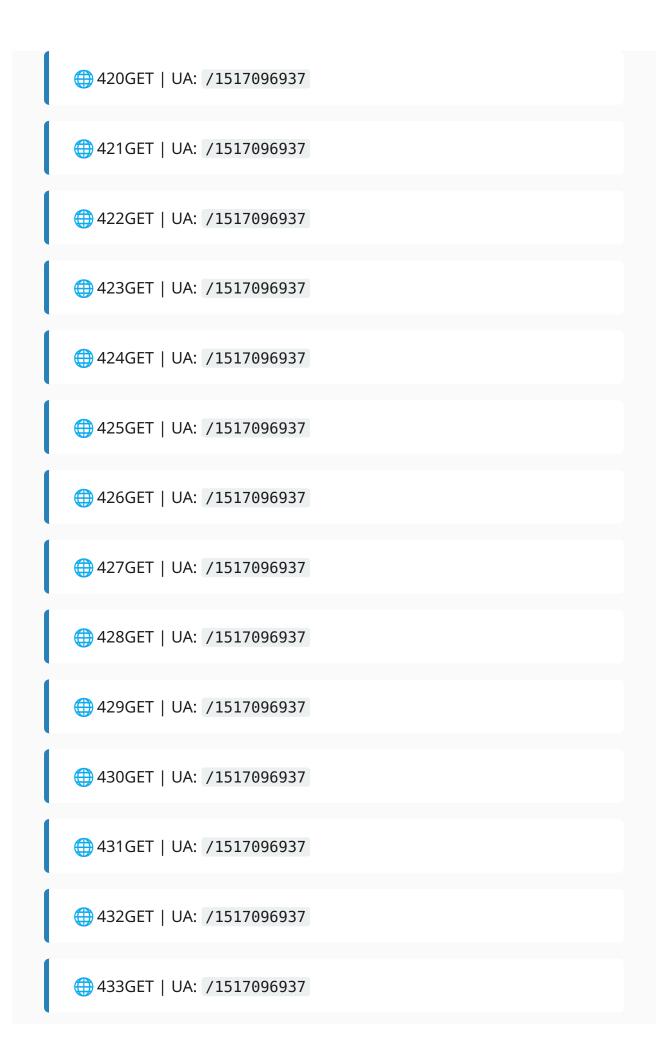


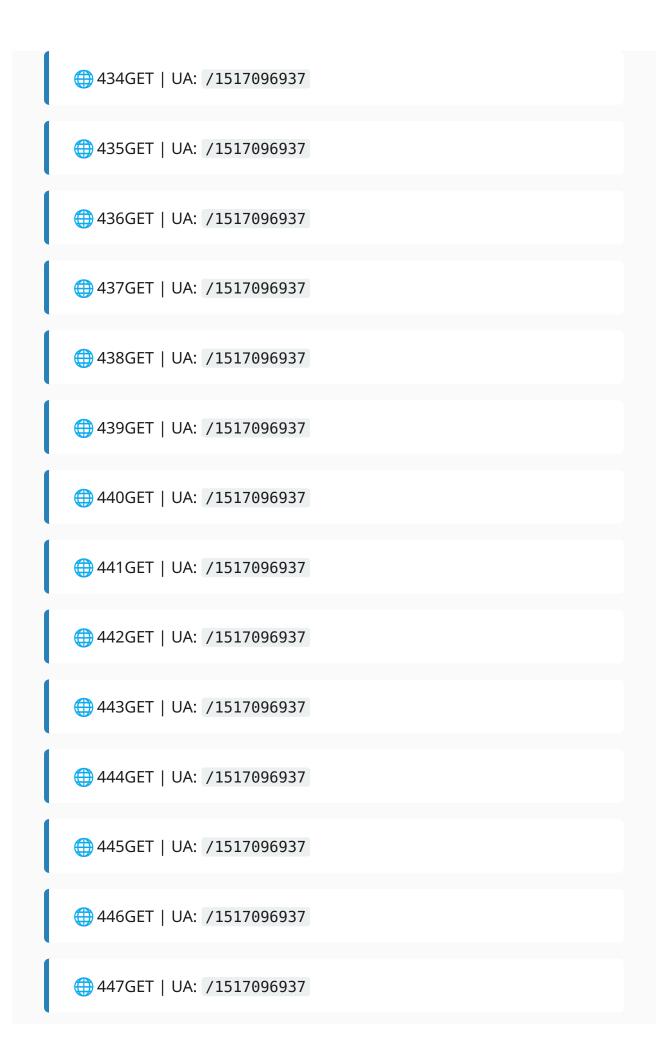


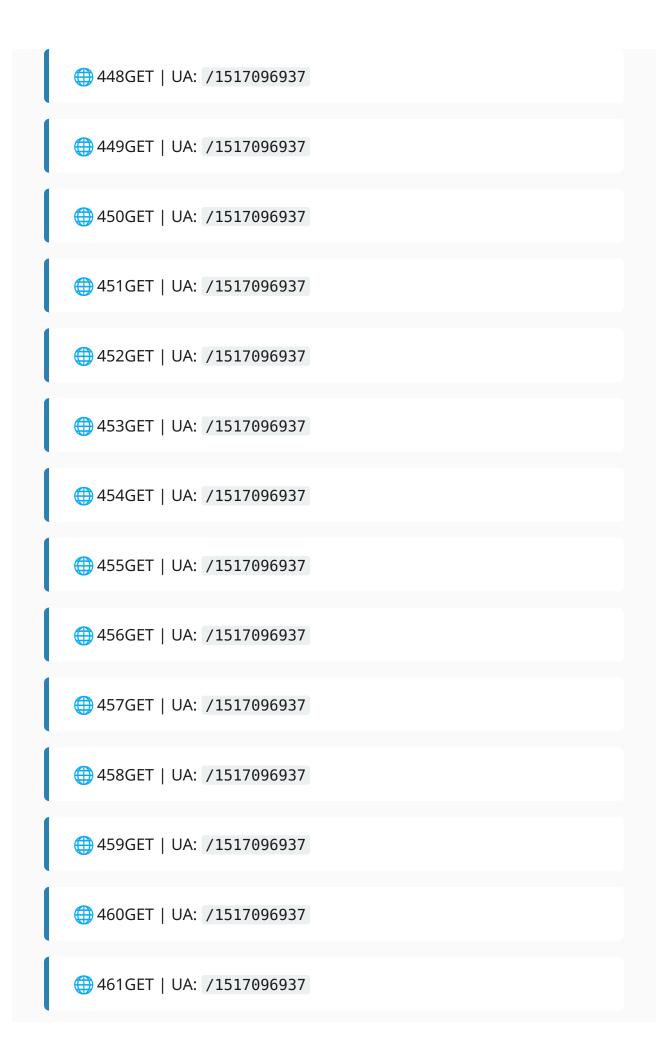
```
( 379GET | UA: /1517096937
380GET | UA: /1517096937?k=script: RunRH, status: OK,
message: PS process started
( 381GET | UA: /1517096937
( 382GET | UA: /1517096937
( 383GET | UA: /1517096937
( 384GET | UA: /1517096937
( 385GET | UA: /1517096937
(m) 386GET | UA: /1517096937
( 387GET | UA: /1517096937
( 388GET | UA: /1517096937
(m) 389GET | UA: /1517096937
( 390GET | UA: /1517096937
(math) 391GET | UA: /1517096937
```

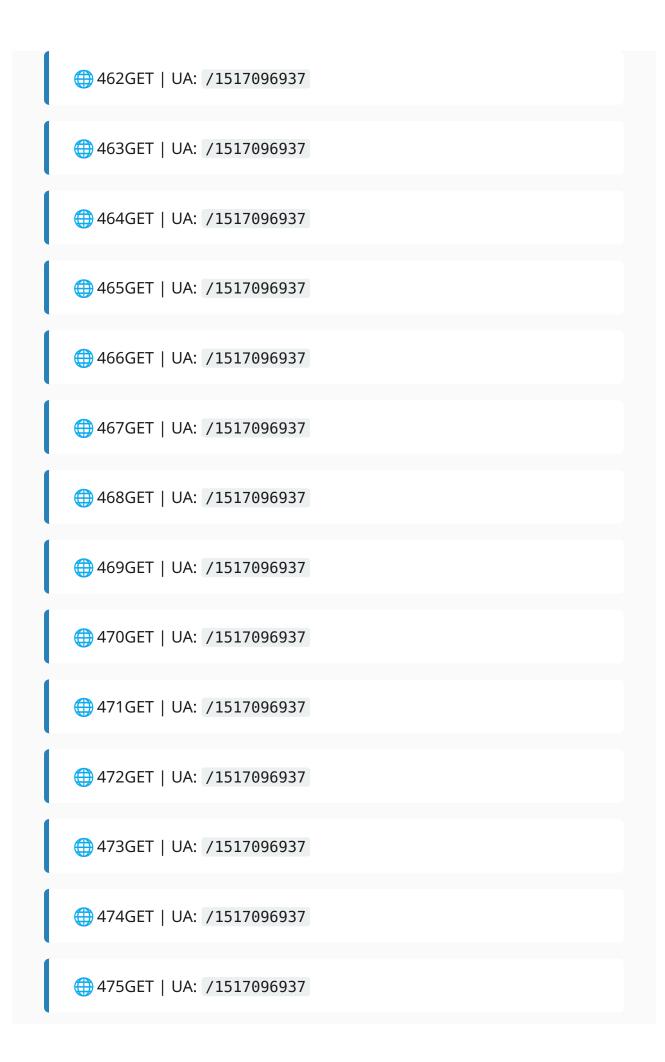


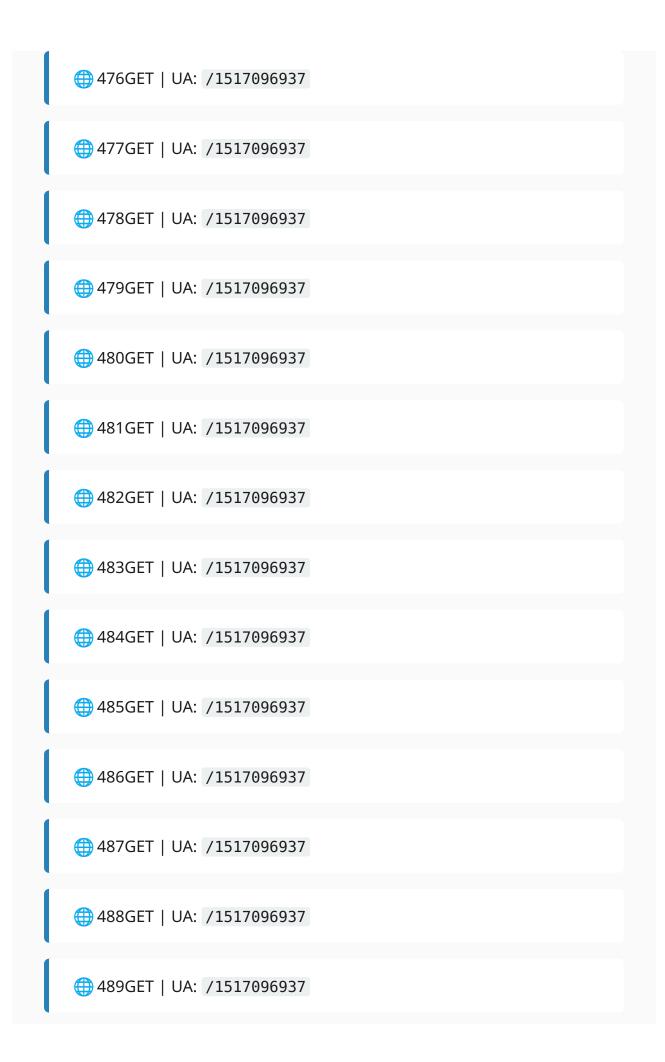


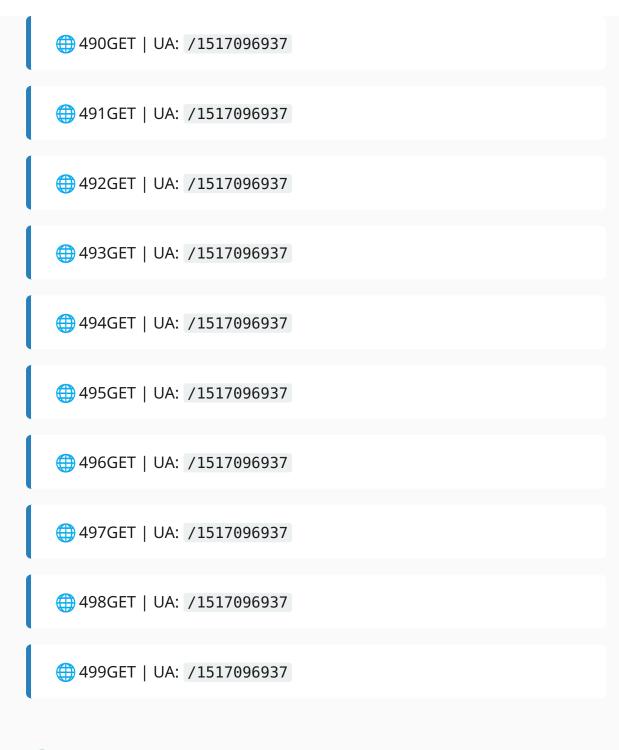












Suricata HTTP Requests

www.msftconnecttest.com/connecttest.txt | UA: Microsoft NCSI

\$\bigoplus 5.252.153.241/api/file/get-file/29842.ps1 | UA: None

```
(math) 5.252.153.241/1517096937 | UA: None
$\begin{aligned}
\begin{aligned}
\begin{aligne
(compatible; MSIE 7.0; Windows NT 10.0; Win64; x64;
Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET
CLR 3.0.30729; .NET CLR 3.5.30729)
 (https://doi.org/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.10
 (mag) 5.252.153.241/1517096937 | UA: None
 ( 5.252.153.241/1517096937 | UA: None
 (iii) 5.252.153.241/1517096937 | UA: None
 (iii) 5.252.153.241/1517096937 | UA: None
 (iii) 5.252.153.241/1517096937 | UA: None
 (mag) 5.252.153.241/1517096937 | UA: None
 (mag) 5.252.153.241/1517096937 | UA: None
 (iii) 5.252.153.241/1517096937 | UA: None
 ( 5.252.153.241/1517096937 | UA: None
 (iii) 5.252.153.241/1517096937 | UA: None
```

- ⊕ 5.252.153.241/1517096937 | UA: None
- # www.msftconnecttest.com/connecttest.txt | UA: Microsoft NCSI
- msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/ files/2ed1297e-f6c9-4355-aec4-433ea371b116? P1=1737884967&P2=404&P3=2&P4=DQ%2frdpZetb6%2bCA7SUqmOgjEUa0b3x%2f0slO | UA: Microsoft BITS/7.8
- msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/
 files/2ed1297e-f6c9-4355-aec4-433ea371b116?
 P1=1737884967&P2=404&P3=2&P4=DQ%2frdpZetb6%2bCA7SUqmOgjEUa0b3x%2f0slO
 | UA: Microsoft BITS/7.8
- master16.teamviewer.com/din.aspx?
 s=91930144&id=0&client=DynGate&p=10000002 | UA: Mozilla/4.0
 (compatible; MSIE 6.0; DynGate)
- (iii) 5.252.153.241/1517096937 | UA: None
- master16.teamviewer.com/din.aspx?
 s=91930119&id=0&client=DynGate&p=10000002 | UA: Mozilla/4.0
 (compatible; MSIE 6.0; DynGate)
- master16.teamviewer.com/din.aspx?
 s=00000000&id=0&client=DynGate&rnd=216758732&p=10000001 |
 UA: Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
- master16.teamviewer.com/din.aspx?
 s=91930165&id=0&client=DynGate&p=10000002 | UA: Mozilla/4.0
 (compatible; MSIE 6.0; DynGate)

master16.teamviewer.com/dout.aspx?
s=91930144&p=10000001&client=DynGate&data=FyQSkgCjHqkys5MkoZ6ZGhycGJuamZ
| UA: Mozilla/4.0 (compatible; MSIE 6.0; DynGate)

msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/
files/2a0d597c-a09c-4400-be86-87596dd2e696?
P1=1737884967&P2=404&P3=2&P4=W7WOpOZ6ahXXhvqsFdcWAJHdZVPv8SRh1FficfbizI
| UA: Microsoft BITS/7.8

master16.teamviewer.com/din.aspx?
s=91930144&id=0&client=DynGate&p=10000002 | UA: Mozilla/4.0
(compatible; MSIE 6.0; DynGate)

master16.teamviewer.com/din.aspx?
s=00000000&id=0&client=DynGate&rnd=427975263&p=10000001 |
UA: Mozilla/4.0 (compatible; MSIE 6.0; DynGate)

msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/ files/2a0d597c-a09c-4400-be86-87596dd2e696? P1=1737884967&P2=404&P3=2&P4=W7WOpOZ6ahXXhvqsFdcWAJHdZVPv8SRh1FficfbizI UA: Microsoft BITS/7.8

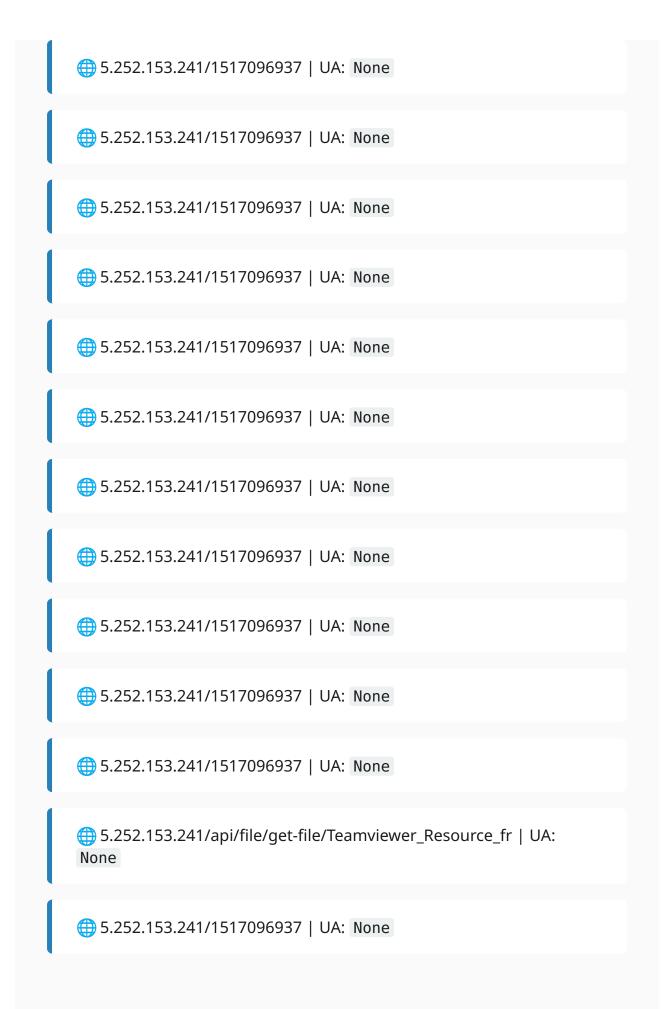
master16.teamviewer.com/dout.aspx?
s=91930119&p=10000001&client=DynGate&data=FyQSkgCjHqkys5MkoZ6ZGhycGJuamZ
| UA: Mozilla/4.0 (compatible; MSIE 6.0; DynGate)

master16.teamviewer.com/din.aspx?
s=91930119&id=0&client=DynGate&p=10000002 | UA: Mozilla/4.0
(compatible; MSIE 6.0; DynGate)

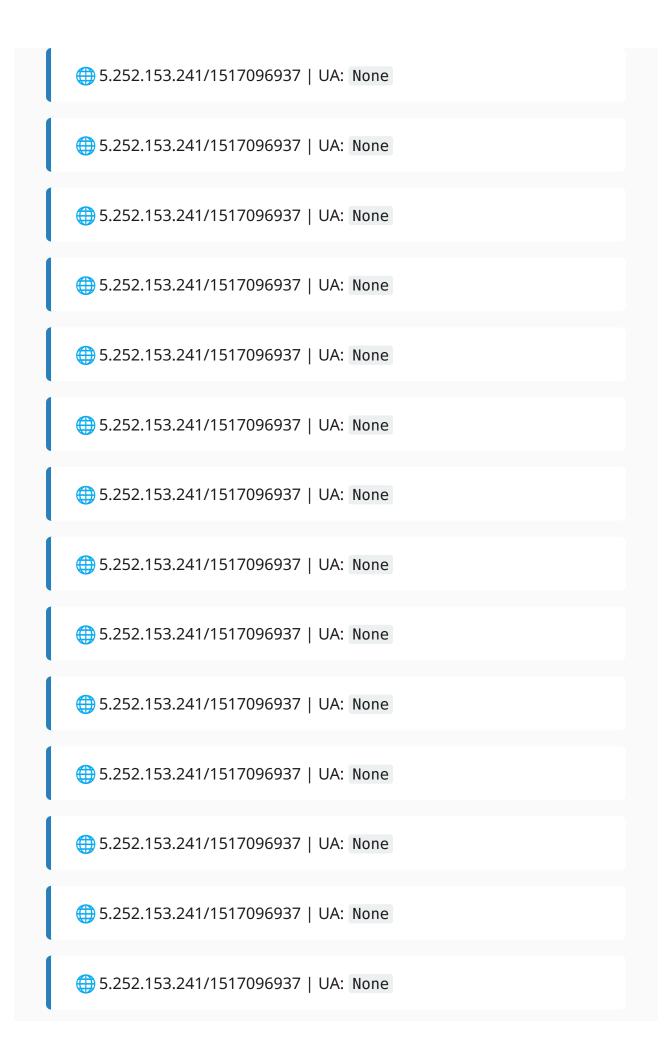
master16.teamviewer.com/din.aspx?
s=91930135&id=0&client=DynGate&p=10000002 | UA: Mozilla/4.0
(compatible; MSIE 6.0; DynGate)

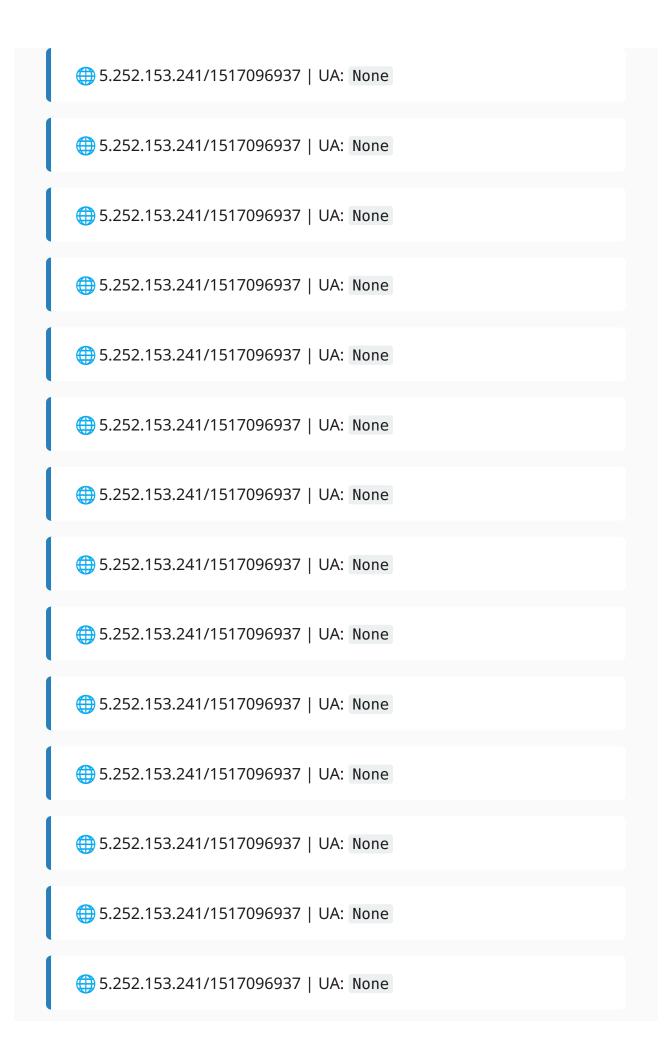
```
(math) 5.252.153.241/1517096937 | UA: None
 master16.teamviewer.com/din.aspx?
s=91930119&id=0&client=DynGate&p=10000002 | UA: Mozilla/4.0
(compatible; MSIE 6.0; DynGate)
 (https://doi.org/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.10
 (iii) 5.252.153.241/1517096937 | UA: None
 master16.teamviewer.com/din.aspx?
s=00000000&id=0&client=DynGate&rnd=418412399&p=10000001 |
UA: Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
 (iii) 5.252.153.241/1517096937 | UA: None
master16.teamviewer.com/dout.aspx?
s=91930165&p=10000001&client=DynGate&data=FyQSkgCjHqkys5MkoZ6ZGhycGJuamZ
 UA: Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
 (https://doi.org/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.10
 master16.teamviewer.com/din.aspx?
s=91930165&id=0&client=DynGate&p=10000002 | UA: Mozilla/4.0
(compatible; MSIE 6.0; DynGate)
 (iii) 5.252.153.241/1517096937 | UA: None
 $\bigoplus 5.252.153.241/api/file/get-file/TeamViewer | UA: None
```

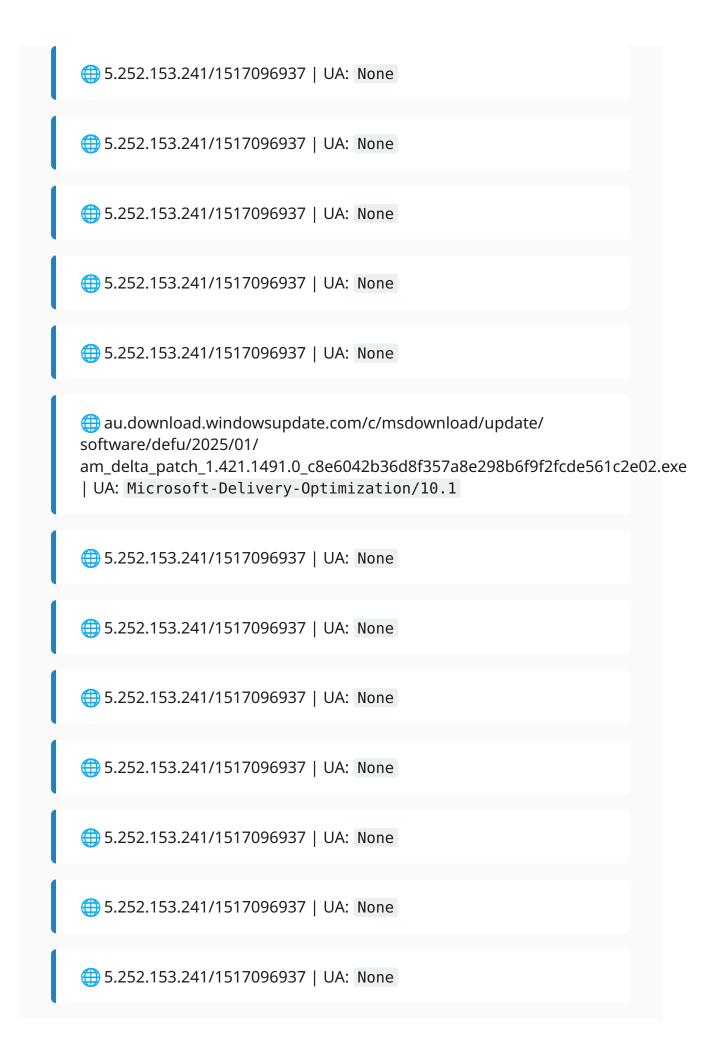
```
(math) 5.252.153.241/1517096937 | UA: None
 (mag) 5.252.153.241/1517096937 | UA: None
 (https://doi.org/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.1016/10.10
 (iii) 5.252.153.241/1517096937 | UA: None
 master16.teamviewer.com/din.aspx?
s=00000000&id=0&client=DynGate&rnd=15187500&p=10000001 |
UA: Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
master16.teamviewer.com/dout.aspx?
s=91930135&p=10000001&client=DynGate&data=FyQSkgCjHqkys5MkoZ6ZGhycGJuamZ
 UA: Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
master16.teamviewer.com/din.aspx?
s=91930135&id=0&client=DynGate&p=10000002 | UA: Mozilla/4.0
(compatible; MSIE 6.0; DynGate)
 master16.teamviewer.com/din.aspx?
s=00000000&id=0&client=DynGate&rnd=5384120&p=10000001 | UA:
Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
master16.teamviewer.com/dout.aspx?
s=91930189&p=10000001&client=DynGate&data=FyQSkgCjHqkys5MkoZ6ZGhycGJuamZ
 UA: Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
 master16.teamviewer.com/din.aspx?
s=91930189&id=0&client=DynGate&p=10000002 | UA: Mozilla/4.0
(compatible; MSIE 6.0; DynGate)
```

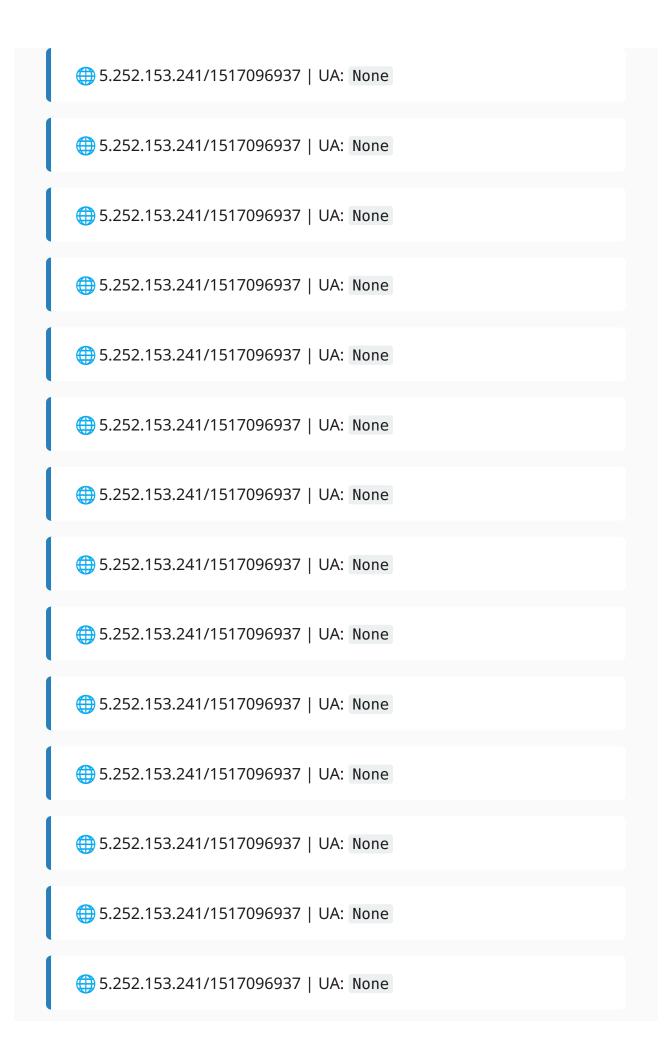


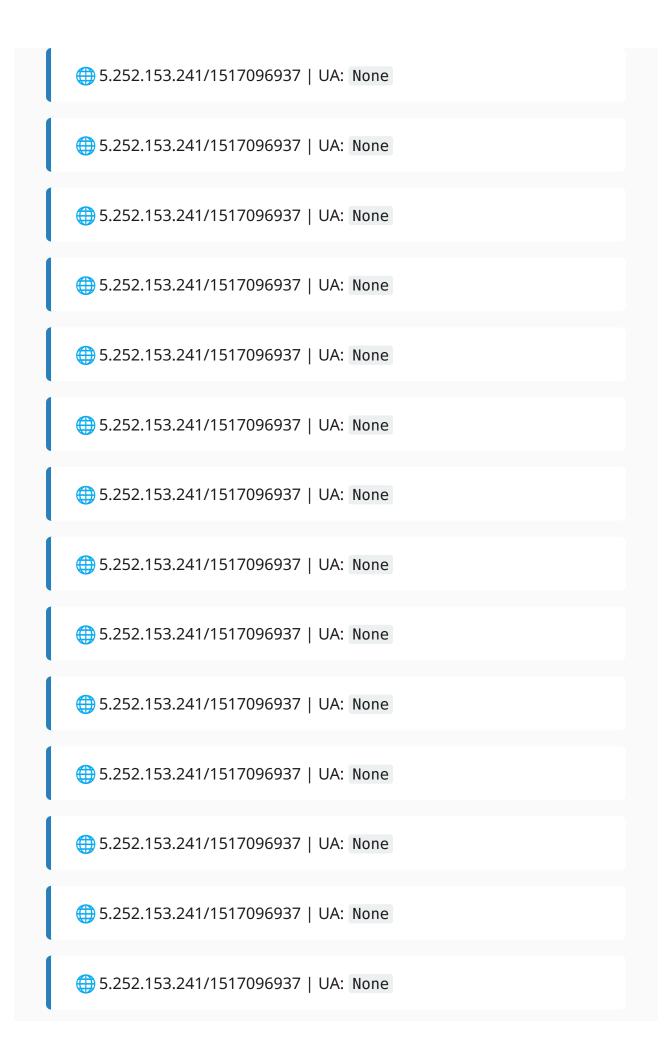
- (5.252.153.241/1517096937 | UA: None
- download.windowsupdate.com/c/msdownload/update/others/
 2025/01/42681409_9e243120ff356d59920855fa02c873fcbcf678c6.cab
 | UA: Windows-Update-Agent/1309.2410.30012.0 ClientProtocol/2.80
- \$ 5.252.153.241/api/file/get-file/TV | UA: None
- (5.252.153.241/1517096937 | UA: None
- (iii) 5.252.153.241/api/file/get-file/pas.ps1 | UA: None
- download.windowsupdate.com/c/msdownload/update/others/
 2025/01/42681408_eba72ad8cac00ea04690b09c0ff175074bb281e9.cab
 | UA: Windows-Update-Agent/1309.2410.30012.0 ClientProtocol/2.80
- ⊕ 5.252.153.241/1517096937 | UA: None
- \$\bigoplus 5.252.153.241/1517096937 | UA: None
- download.windowsupdate.com/c/msdownload/update/others/
 2025/01/42681502_106431d428d2c49b06bf00d7ab662ff53edb4726.cab
 | UA: Windows-Update-Agent/1309.2410.30012.0 ClientProtocol/2.80

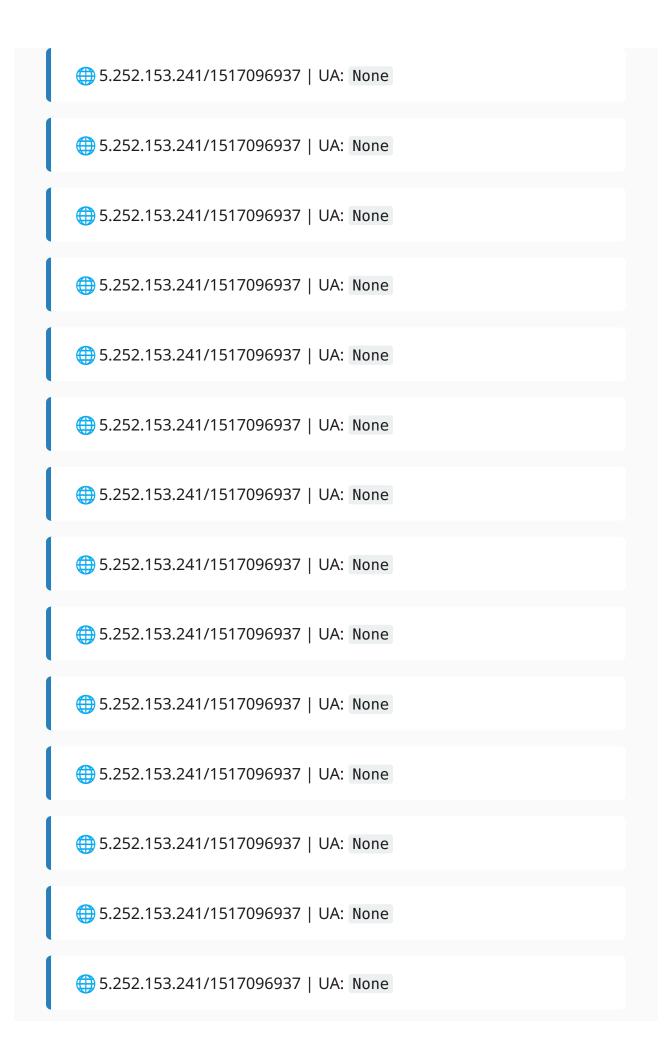


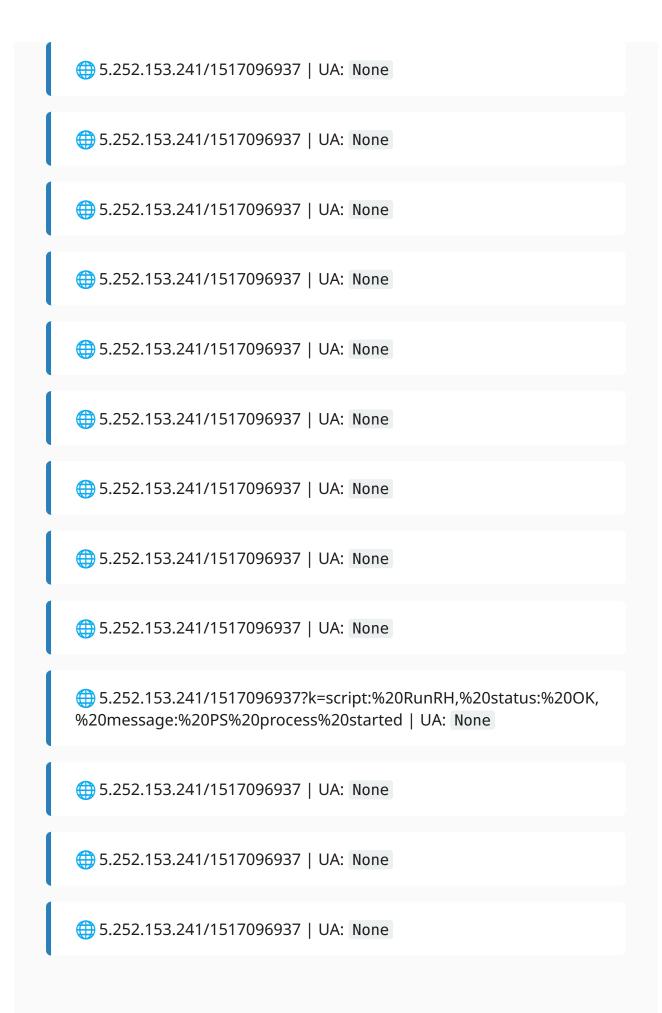


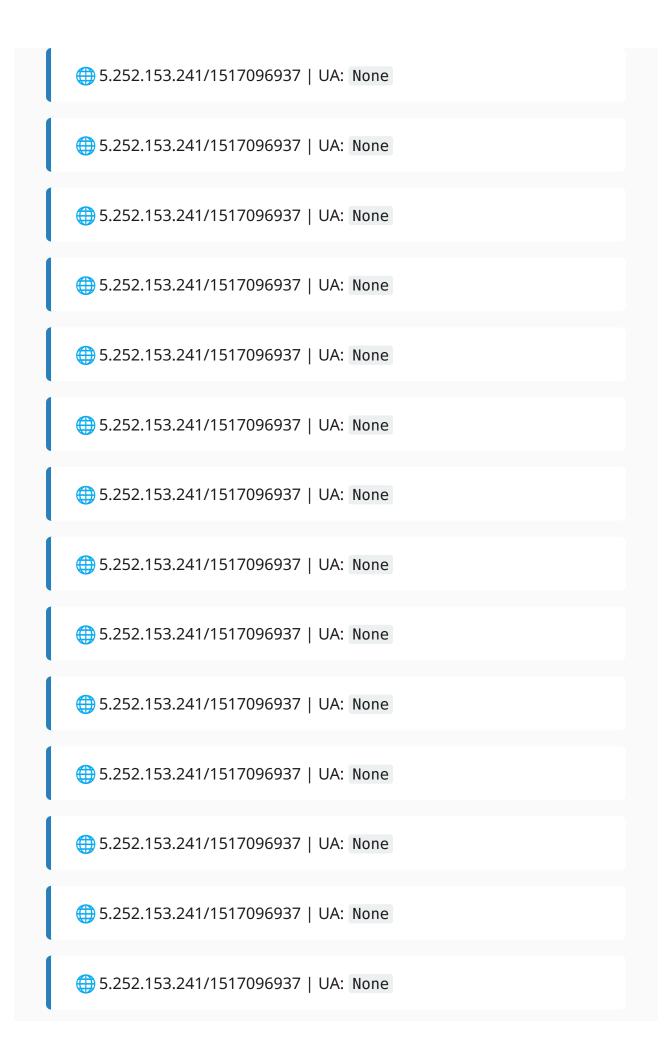


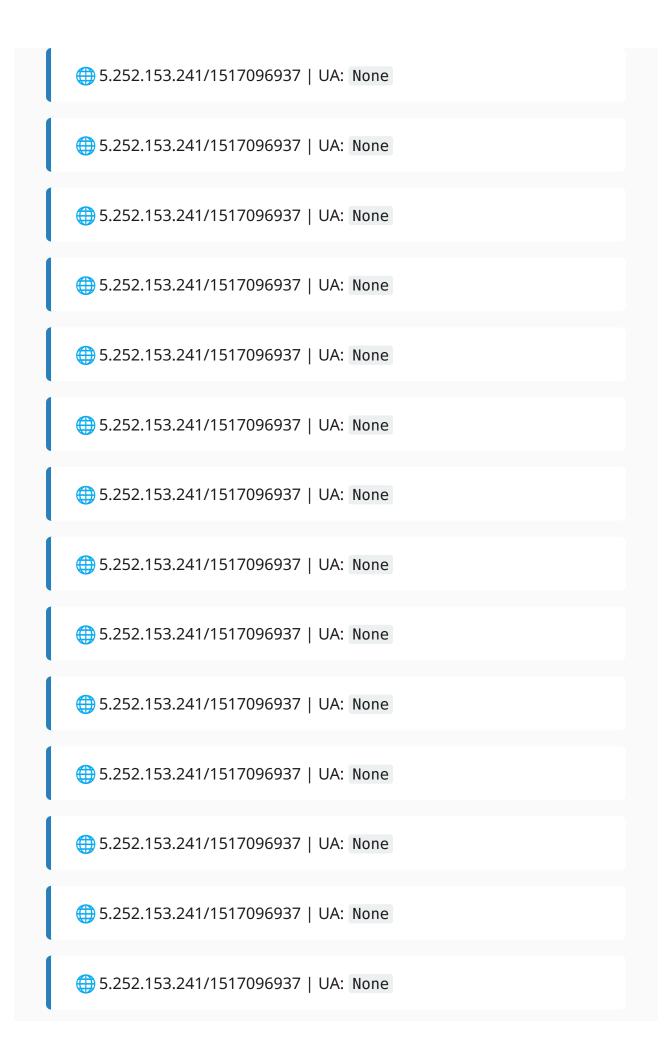




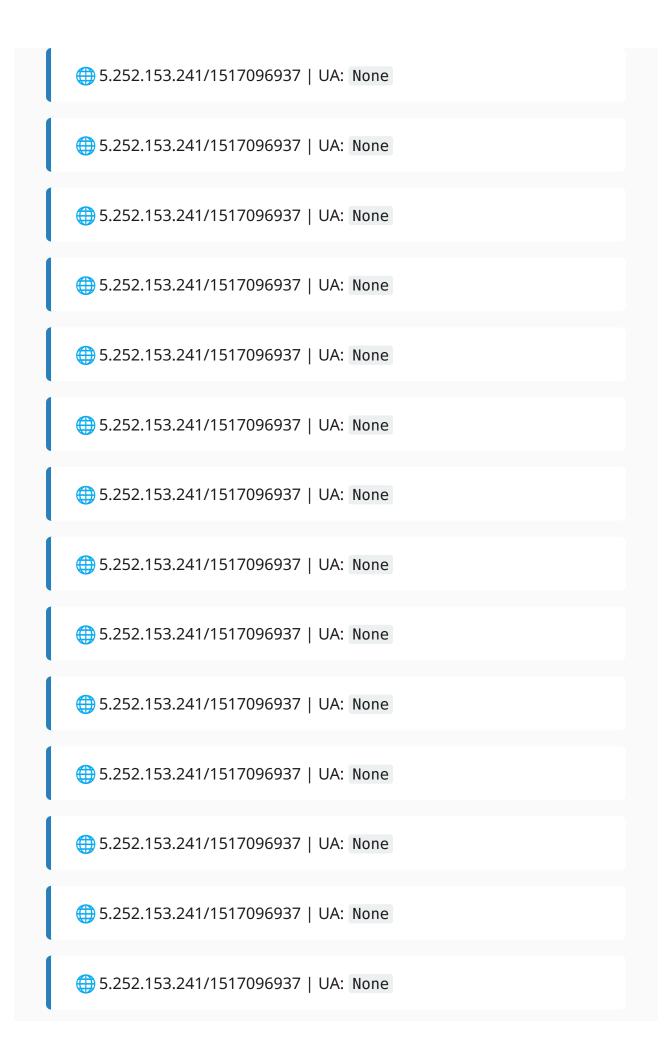


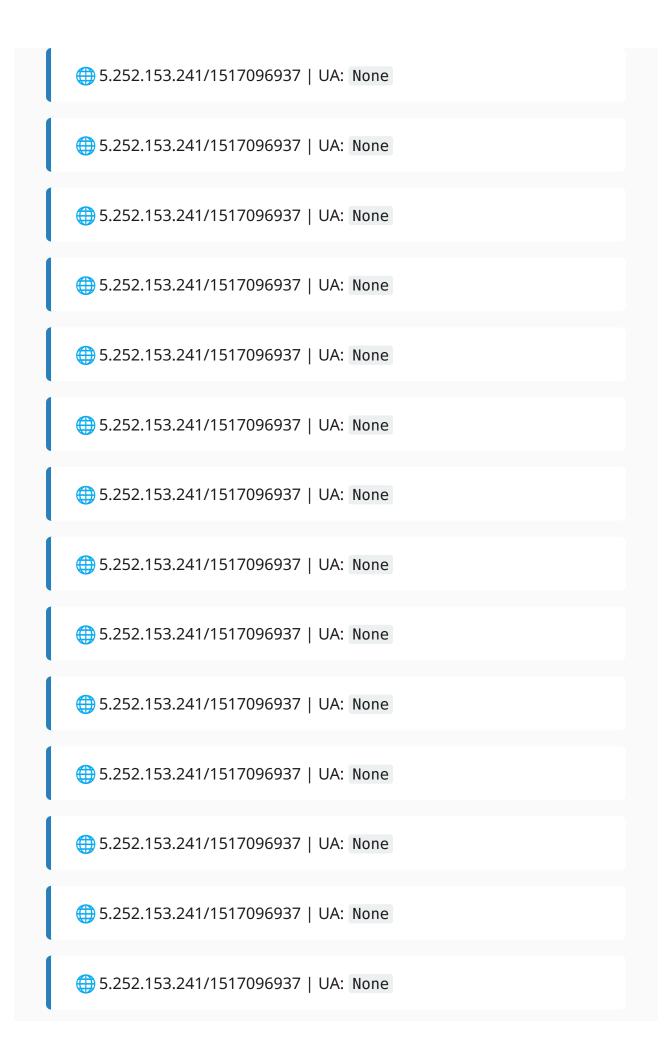


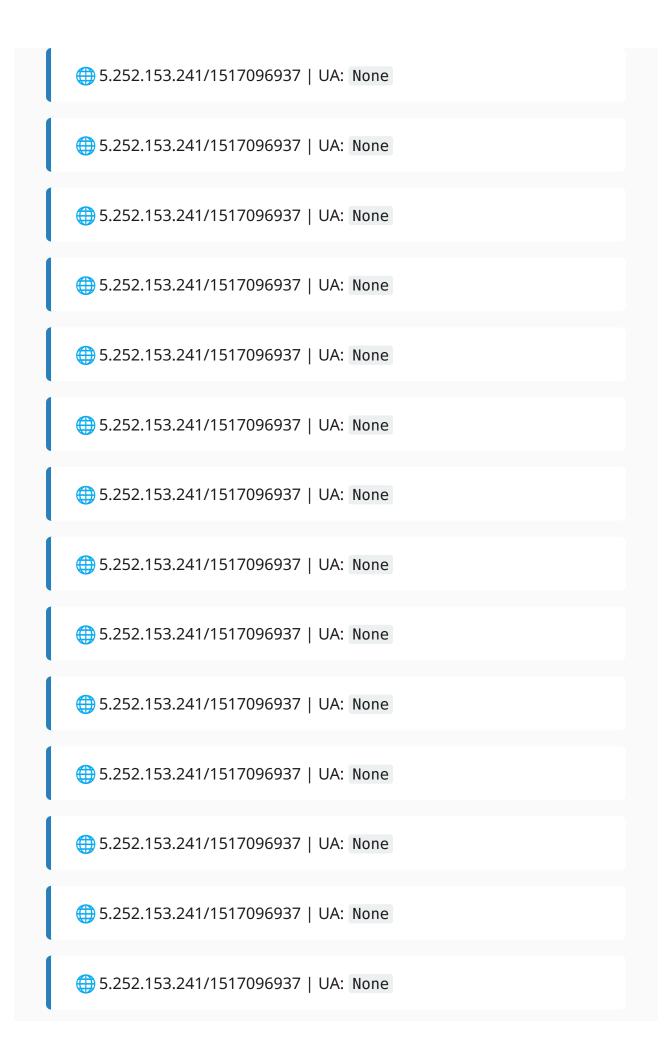


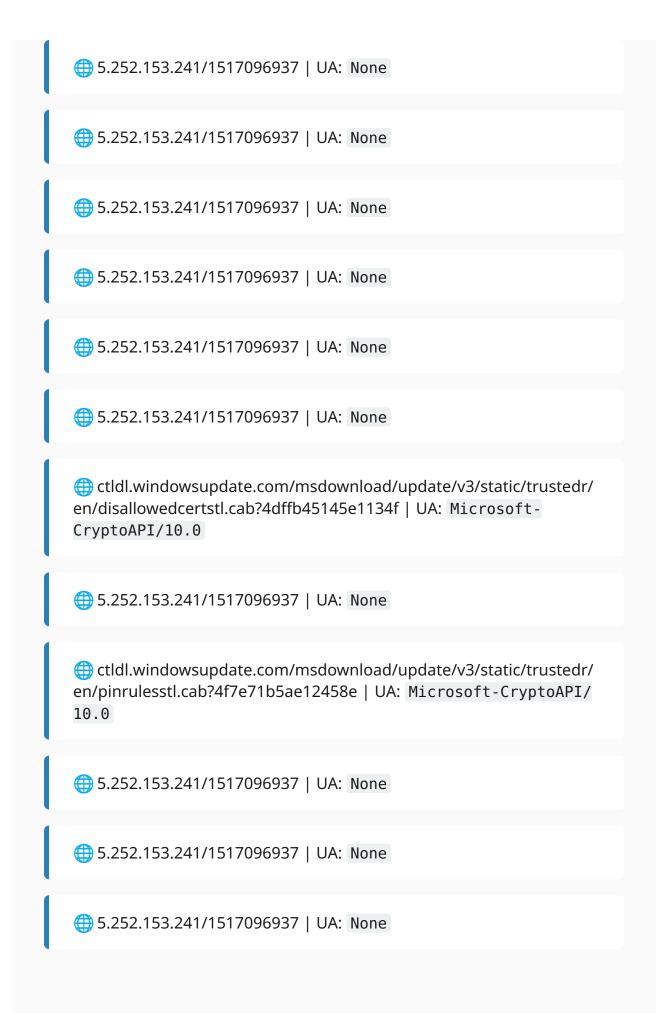


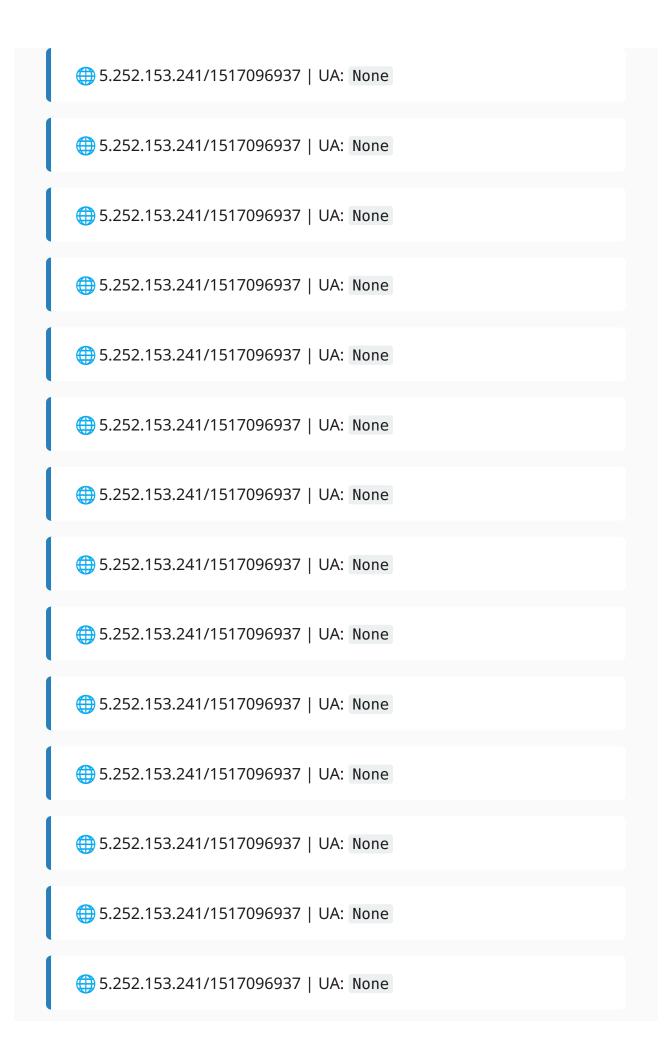
```
master16.teamviewer.com/din.aspx?
s=91930189&id=0&client=DynGate&p=10000002 | UA: Mozilla/4.0
(compatible; MSIE 6.0; DynGate)
( 5.252.153.241/1517096937 | UA: None
( 5.252.153.241/1517096937 | UA: None
(iii) 5.252.153.241/1517096937 | UA: None
( 5.252.153.241/1517096937 | UA: None
( 5.252.153.241/1517096937 | UA: None
(mag) 5.252.153.241/1517096937 | UA: None
(f) 5.252.153.241/1517096937 | UA: None
(iii) 5.252.153.241/1517096937 | UA: None
( 5.252.153.241/1517096937 | UA: None
(mag) 5.252.153.241/1517096937 | UA: None
(mag) 5.252.153.241/1517096937 | UA: None
(m) 5.252.153.241/1517096937 | UA: None
```

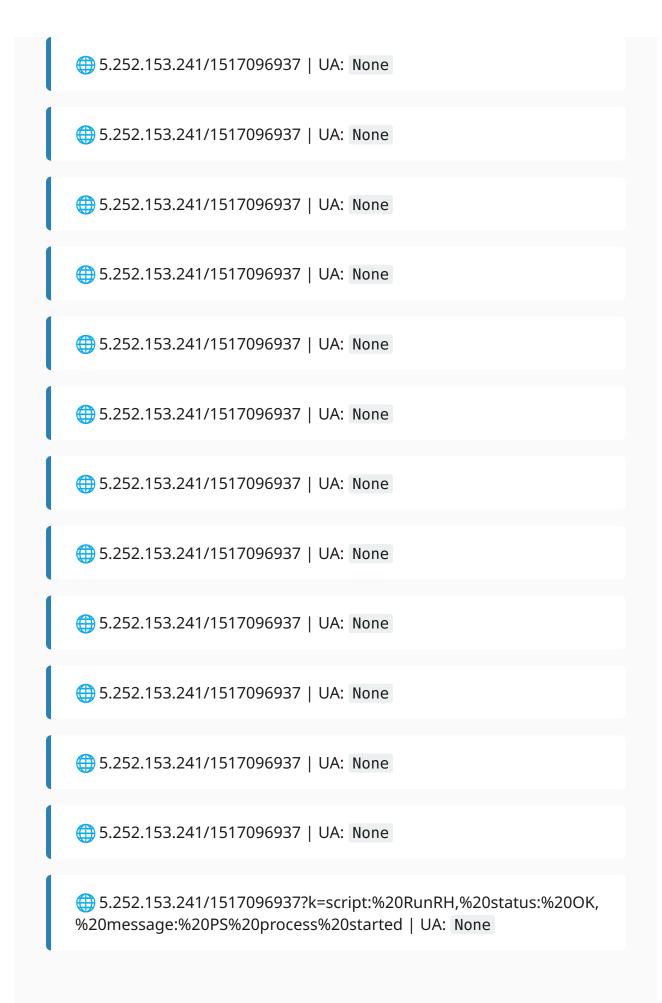


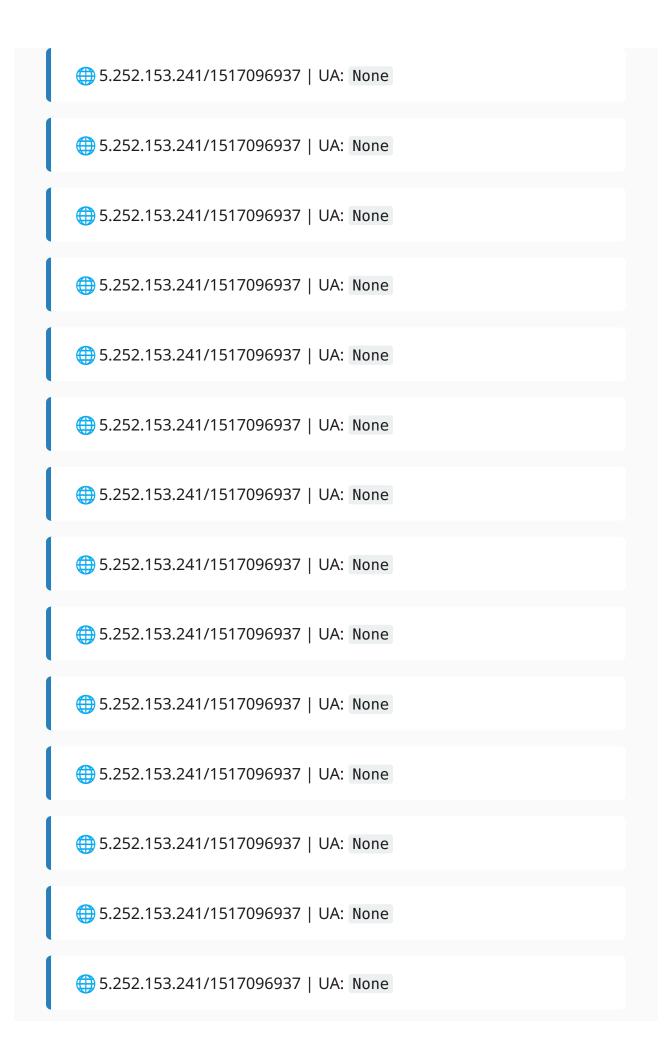


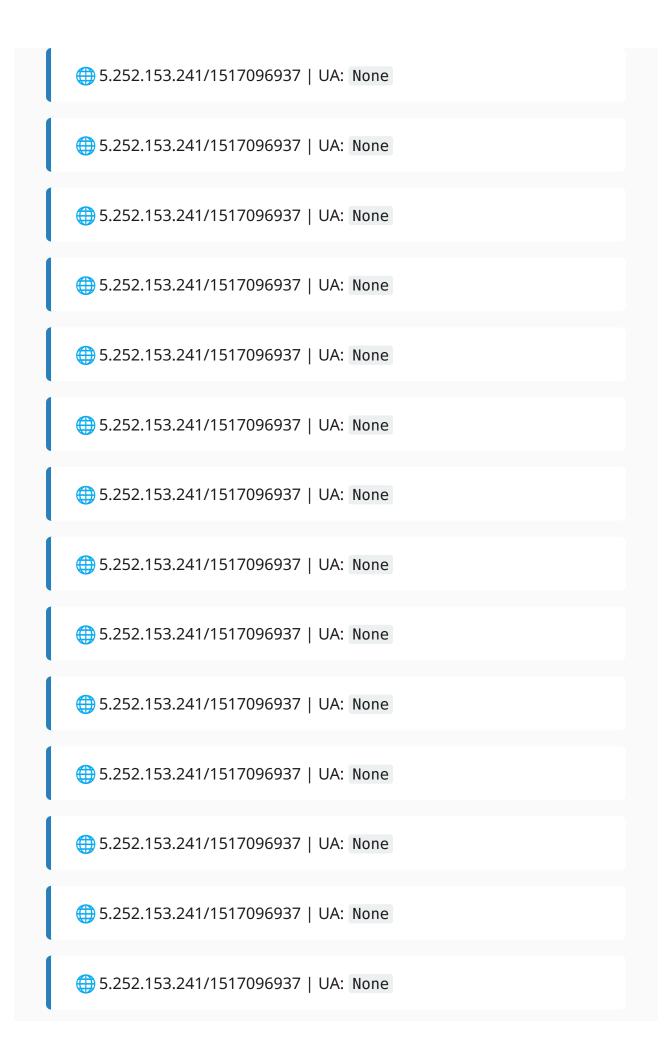


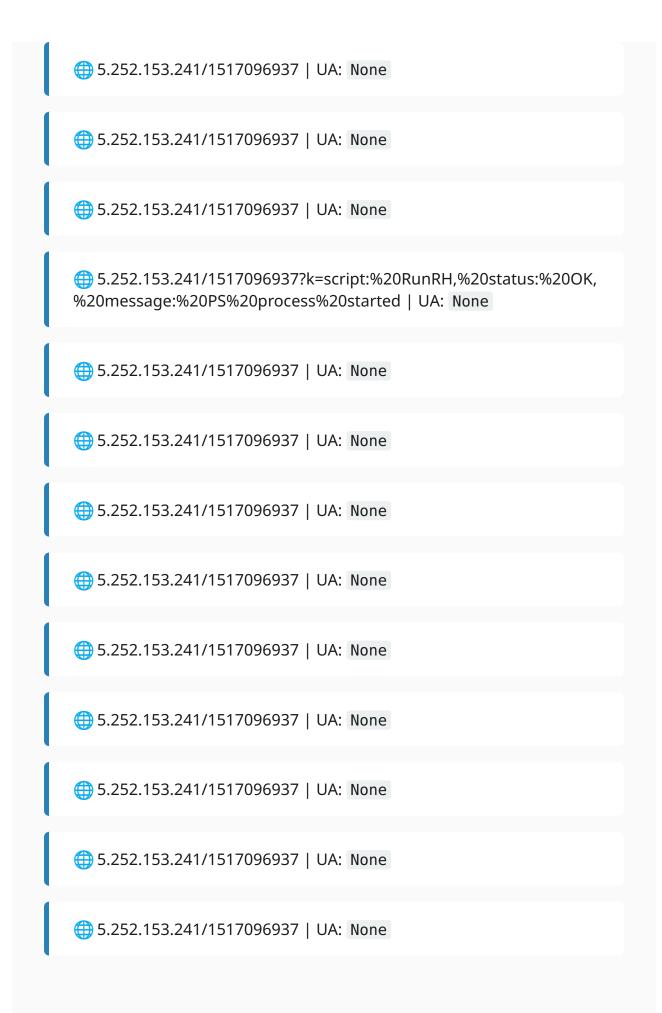


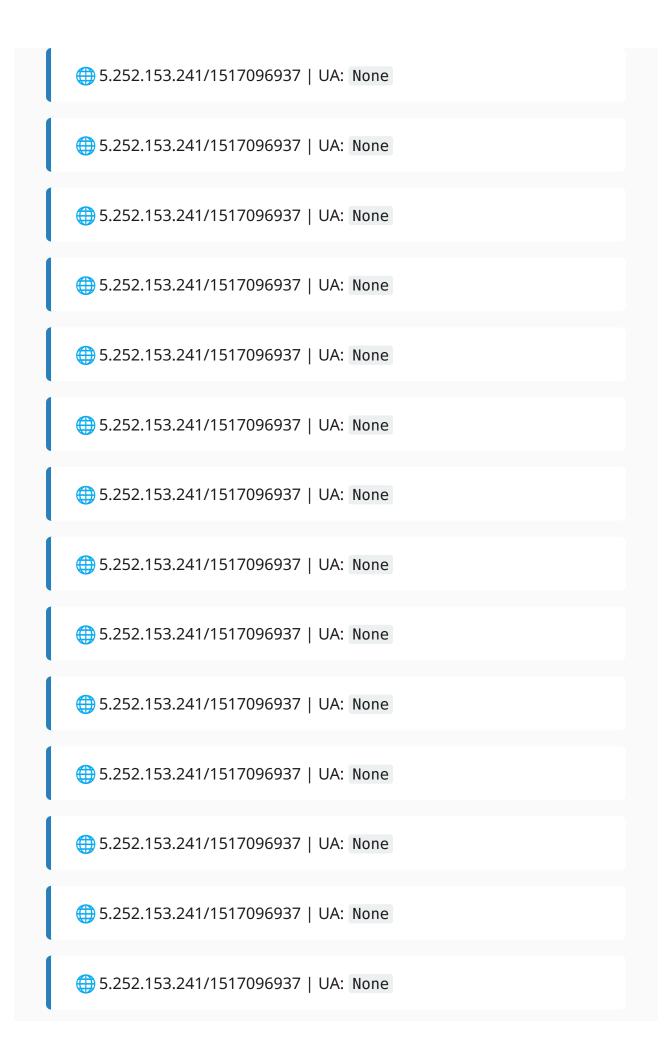


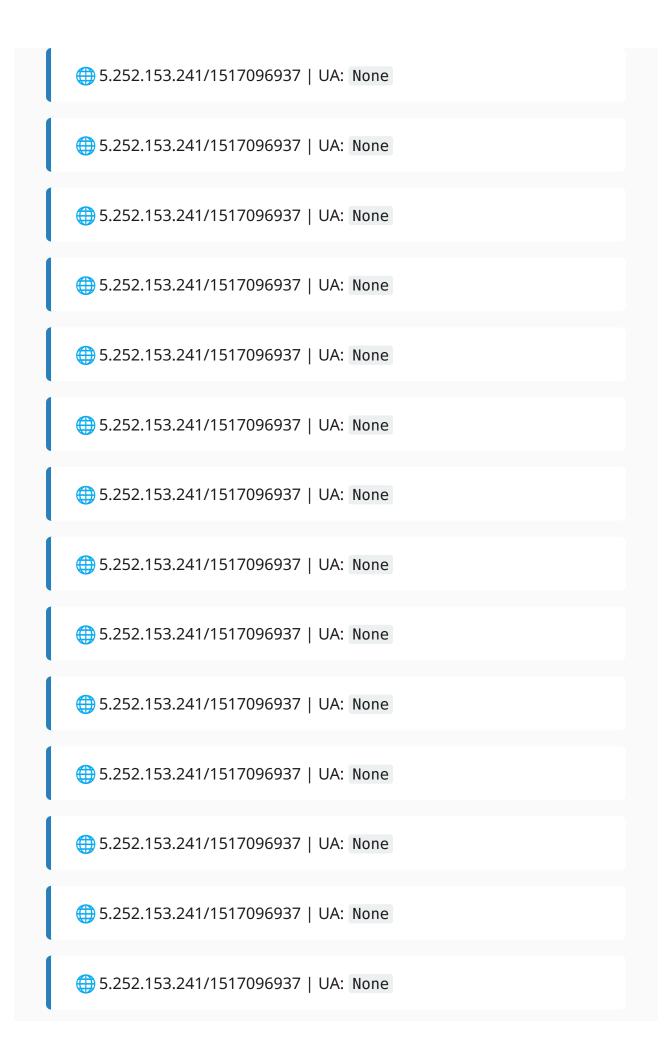


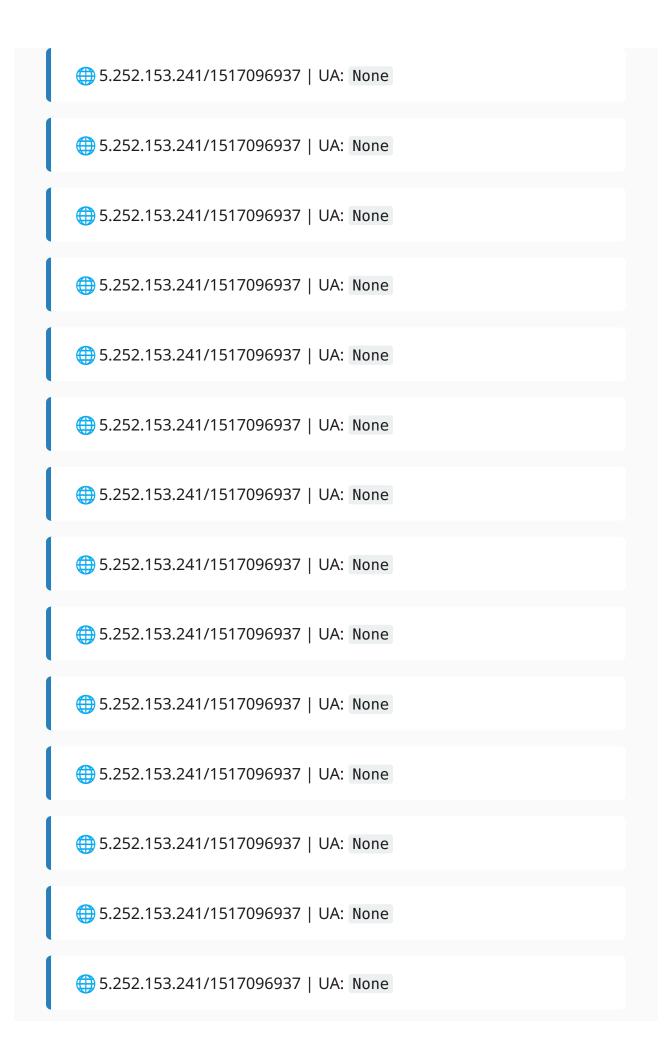


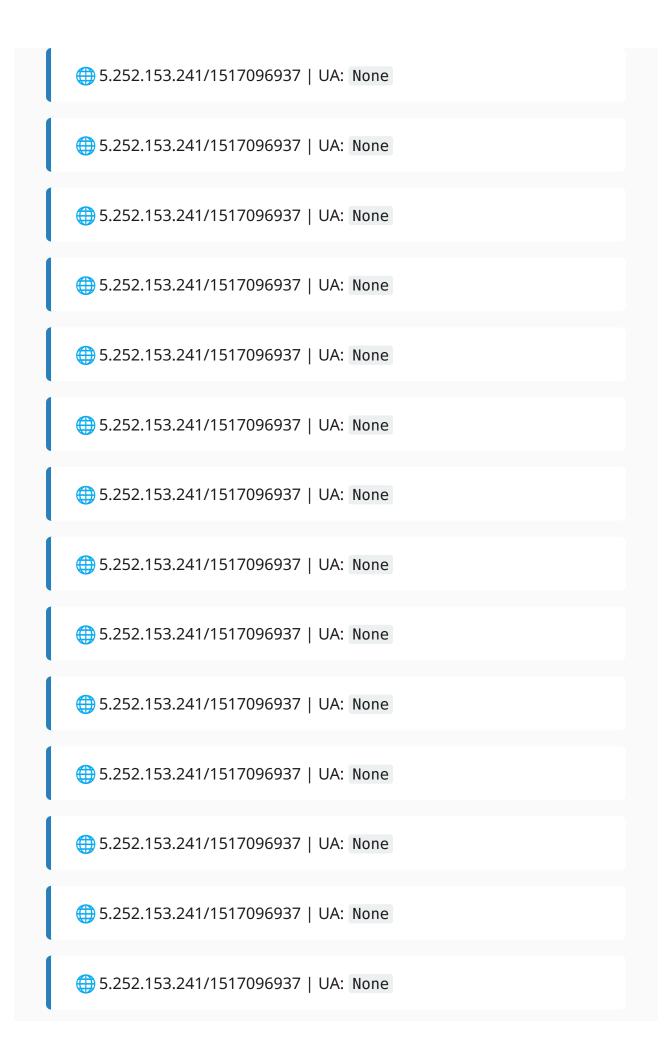


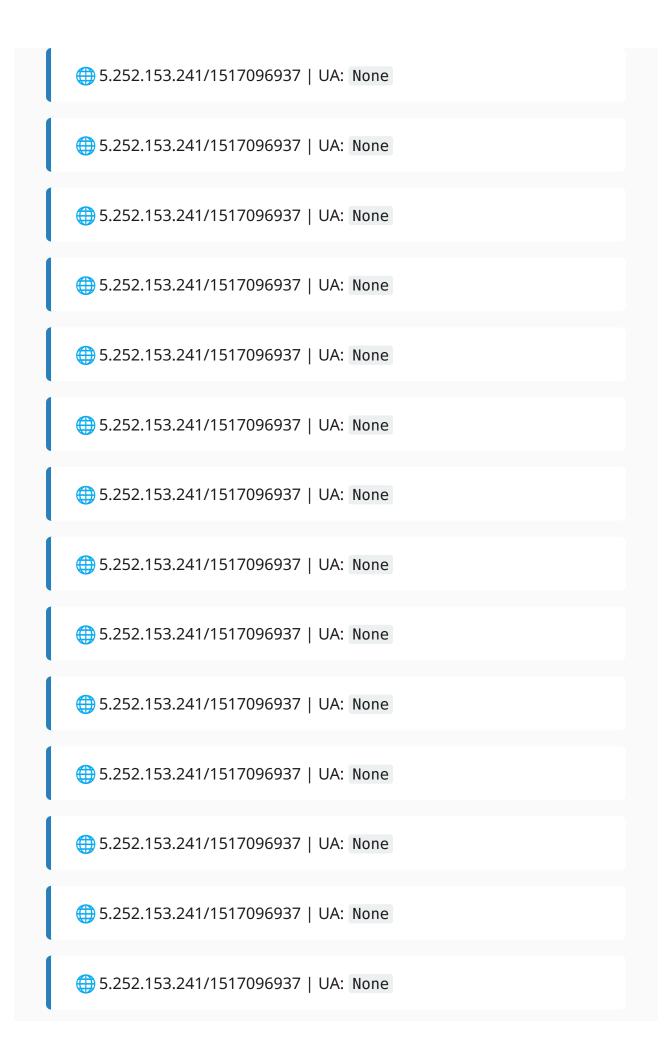


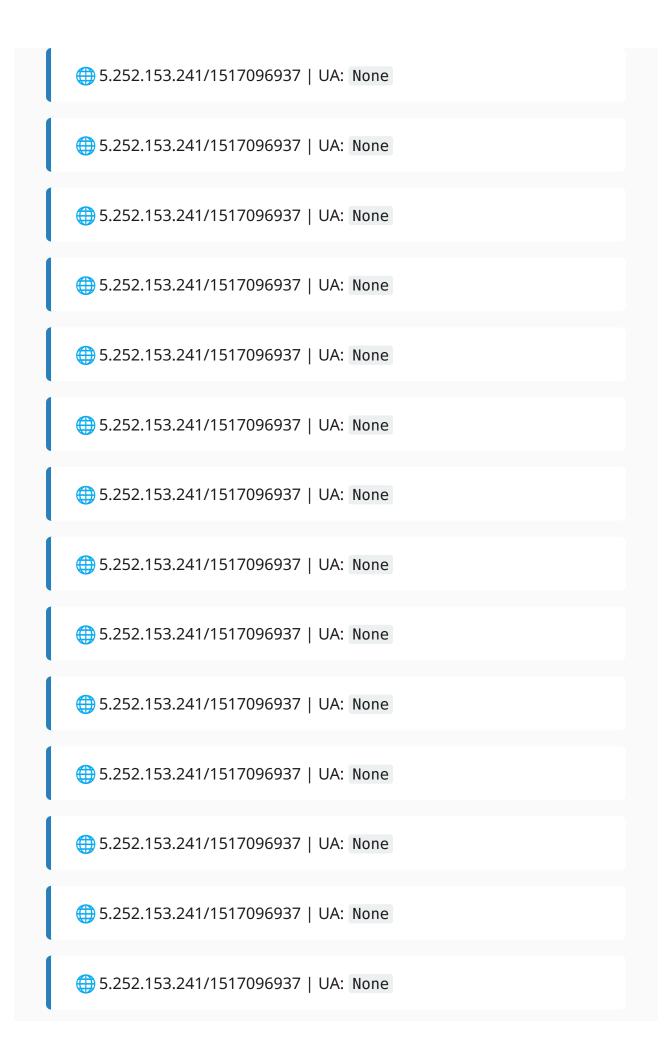


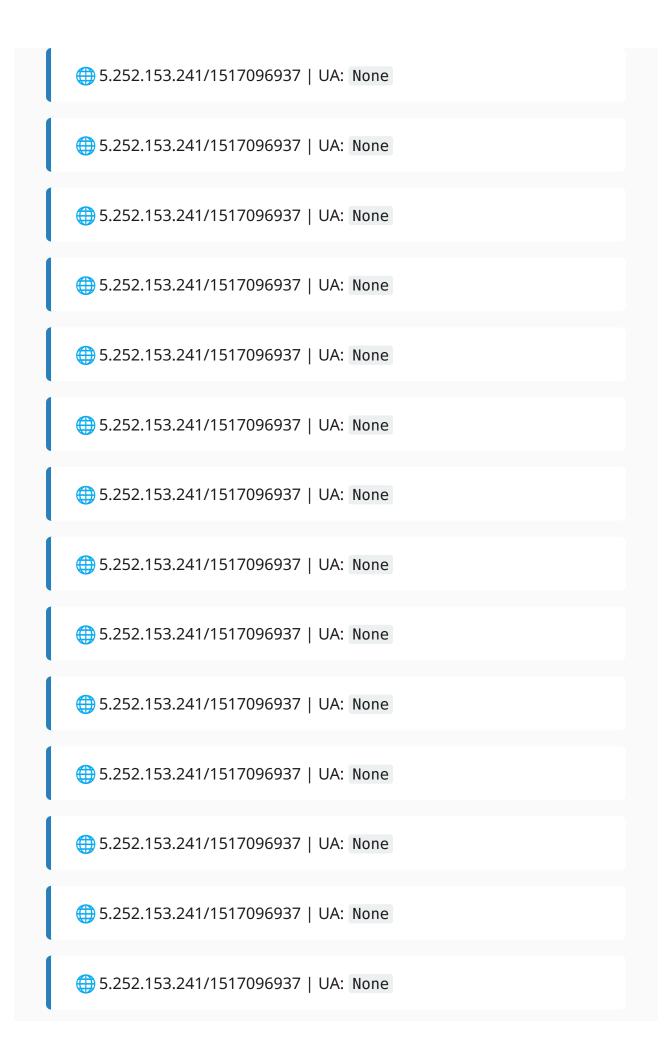


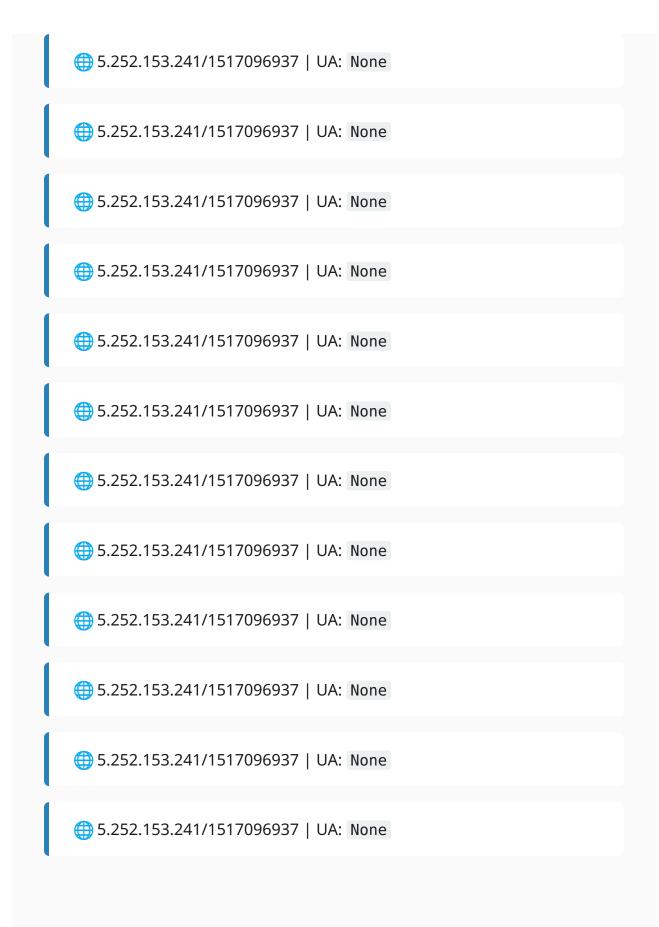












DHCP Hostnames

■ 10.1.17.2 | C1DKej3Kg0eVIhWTc,CZKyUb4VhqTzT2QQ49 →
10.1.17.215

Transferred Files

- application/ocsp-response | Type: | SHA1: F
 - text/plain | Type: | SHA1: F
- application/ocsp-response | Type: | SHA1: F
- application/ocsp-response | Type: | SHA1: F
 - application/ocsp-response | Type: | SHA1: F
 - application/ocsp-response | Type: | SHA1: F
 - application/ocsp-response | Type: | SHA1: F
 - application/ocsp-response | Type: | SHA1: F
 - application/ocsp-response | Type: | SHA1: F
 - text/plain | Type: | SHA1: F

```
text/plain | Type: - | SHA1: F
- | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
- | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
- | Type: - | SHA1: F
- | Type: - | SHA1: F
- | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
application/chrome-ext | Type: - | SHA1: F
- | Type: - | SHA1: F
application/chrome-ext | Type:- | SHA1: F
```

```
- | Type: - | SHA1: F
text/plain | Type: - | SHA1: F
application/x-dosexec | Type: - | SHA1: F
application/x-dosexec | Type: - | SHA1: F
application/x-dosexec | Type: - | SHA1: F
text/plain | Type: - | SHA1: F
- | Type: - | SHA1: F
- | Type: - | SHA1: F
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
- | Type: - | SHA1: F
- | Type: - | SHA1: F
text/plain | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
- | Type: - | SHA1: F
- | Type: - | SHA1: F
- | Type: - | SHA1: F
text/html | Type: - | SHA1: F
- | Type: - | SHA1: F
- | Type: - | SHA1: F
text/html | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
- | Type: - | SHA1: F
text/html | Type: - | SHA1: F
- | Type: - | SHA1: F
📁 - | Type: - | SHA1: F
text/html | Type: - | SHA1: F
- | Type: - | SHA1: F
- | Type: - | SHA1: F
text/html | Type: - | SHA1: F
- | Type: - | SHA1: F
- | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
```

```
application/ocsp-response | Type: - | SHA1: F
application/ocsp-response | Type:- | SHA1: F
```

```
application/ocsp-response | Type: - | SHA1: F
- | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
text/plain | Type: - | SHA1: F
- | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
application/vnd.ms-cab-compressed | Type: - | SHA1: F
application/vnd.ms-cab-compressed | Type: - | SHA1: F
application/vnd.ms-cab-compressed | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
application/x-dosexec | Type: - | SHA1: F
- | Type: - | SHA1: F
- | Type: - | SHA1: F
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
text/plain | Type: - | SHA1: F
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
- | Type: - | SHA1: F
- | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
text/plain | Type: - | SHA1: F
- | Type: - | SHA1: F
- | Type: - | SHA1: F
- | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
📁 - | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
application/ocsp-response | Type: - | SHA1: F
- | Type: - | SHA1: F
```

```
application/ocsp-response | Type:-| SHA1: F
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
```

```
- | Type: - | SHA1: F
   - | Type: - | SHA1: F
SSL/TLS Sessions (Zeek)
  SNI: secp256r1 | Subject:
  kv801.prod.do.dsp.mp.microsoft.com
   🔑 SNI: secp384r1 | Subject:
   geo.prod.do.dsp.mp.microsoft.com
   SNI: secp384r1 | Subject: client.wns.windows.com
   SNI: secp384r1 | Subject: v10.events.data.microsoft.com
   SNI: secp384r1 | Subject: v20.events.data.microsoft.com
   SNI: secp384r1 | Subject: windows.msn.com
```

```
SNI: secp384r1 | Subject: officeclient.microsoft.com
SNI: secp384r1 | Subject: www.msn.com
SNI: x25519 | Subject: www.bing.com
SNI: secp384r1 | Subject: odc.officeapps.live.com
SNI: x25519 | Subject: assets.msn.com
SNI: secp384r1 | Subject: odc.officeapps.live.com
SNI: x25519 | Subject: g.live.com
SNI: secp256r1 | Subject: oneclient.sfx.ms
SNI: secp256r1 | Subject: services.gfe.nvidia.com
SNI: secp384r1 | Subject: edge.microsoft.com
SNI: secp256r1 | Subject: static.edge.microsoftapp.net
SNI: secp384r1 | Subject: ntp.msn.com
SNI: secp256r1 | Subject: services.gfe.nvidia.com
SNI: x25519 | Subject: assets.msn.com
```

```
SNI: x25519 | Subject: assets.msn.com
SNI: secp384r1 | Subject: login.microsoftonline.com
SNI: x25519 | Subject: c.msn.com
SNI: secp384r1 | Subject: browser.events.data.msn.com
SNI: secp384r1 | Subject: browser.events.data.msn.com
SNI: x25519 | Subject: www.bing.com
SNI: x25519 | Subject: www.bing.com
SNI: secp384r1 | Subject: edge.microsoft.com
SNI: secp384r1 | Subject: browser.events.data.msn.com
SNI: x25519 | Subject: www.bing.com
SNI: x25519 | Subject: r.bing.com
SNI: secp384r1 | Subject: browser.events.data.msn.com
SNI: secp384r1 | Subject: edge.microsoft.com
SNI: secp384r1 | Subject: edge.microsoft.com
```

```
SNI: unknown-4588 | Subject: google-
authenticator.burleson-appliance.net
SNI: x25519 | Subject: authenticatoor.org
SNI: secp384r1 | Subject: login.microsoftonline.com
SNI: x25519 | Subject: appointedtimeagriculture.com
SNI: secp256r1 | Subject: edge-consumer-
static.azureedge.net
SNI: x25519 | Subject: checkappexec.microsoft.com
SNI: x25519 | Subject: azure.microsoft.com
SNI: x25519 | Subject: www.microsoft.com
```

```
SNI: x25519 | Subject: www.microsoft.com
SNI: x25519 | Subject: play.vidyard.com
SNI: x25519 | Subject: c.go-mpulse.net
SNI: x25519 | Subject: publisher.liveperson.net
SNI: x25519 | Subject: lpcdn.lpsnmedia.net
SNI: x25519 | Subject: cdn-dynmedia-1.microsoft.com
SNI: secp256r1 | Subject: js.monitor.azure.com
SNI: secp256r1 | Subject: lptag.liveperson.net
SNI: x25519 | Subject: assets.adobedtm.com
🔑 SNI: secp384r1 | Subject:
browser.events.data.microsoft.com
SNI: secp384r1 | Subject:
browser.events.data.microsoft.com
SNI: secp256r1 | Subject: accdn.lpsnmedia.net
SNI: x25519 | Subject: c1.microsoft.com
```

```
SNI: x25519 | Subject: dpm.demdex.net
SNI: secp384r1 | Subject: c.bing.com
SNI: x25519 | Subject: mscom.demdex.net
SNI: x25519 | Subject: www.facebook.com
SNI: unknown-4588 | Subject: googleads.g.doubleclick.net
SNI: secp384r1 | Subject: bat.bing.com
SNI: secp384r1 | Subject: dc.ads.linkedin.com
SNI: secp256r1 | Subject: www.clarity.ms
SNI: unknown-4588 | Subject: www.google.com
SNI: secp256r1 | Subject: va.v.liveperson.net
SNI: x25519 | Subject: i.clarity.ms
SNI: x25519 | Subject: cms.analytics.yahoo.com
SNI: secp256r1 | Subject: px.owneriq.net
SNI: - | Subject: px.owneriq.net
```

```
SNI: unknown-4588 | Subject: ds.reson8.com
SNI: secp256r1 | Subject: jadserve.postrelease.com
SNI: secp256r1 | Subject: bttrack.com
SNI: x25519 | Subject: dmpsync.3lift.com
SNI: secp256r1 | Subject: ag.innovid.com
SNI: secp384r1 | Subject: edge.microsoft.com
SNI: secp384r1 | Subject: windows.msn.com
SNI: secp384r1 | Subject: windows.msn.com
SNI: secp384r1 | Subject: www.msn.com
SNI: secp384r1 | Subject: api.msn.com
SNI: secp384r1 | Subject: srtb.msn.com
SNI: x25519 | Subject: img-s-msn-com.akamaized.net
SNI: x25519 | Subject: th.bing.com
SNI: secp384r1 | Subject: login.microsoftonline.com
```

```
SNI: secp384r1 | Subject: settings-win.data.microsoft.com
SNI: x25519 | Subject: www.bing.com
SNI: secp384r1 | Subject: fd.api.iris.microsoft.com
SNI: secp384r1 | Subject: login.microsoftonline.com
🔑 SNI: secp384r1 | Subject:
array804.prod.do.dsp.mp.microsoft.com
🔑 SNI: secp256r1 | Subject:
kv801.prod.do.dsp.mp.microsoft.com
SNI: x25519 | Subject: www.bing.com
SNI: secp384r1 | Subject: login.microsoftonline.com
SNI: secp384r1 | Subject: v20.events.data.microsoft.com
SNI: secp384r1 | Subject: officeclient.microsoft.com
SNI: secp384r1 | Subject: client.wns.windows.com
SNI: secp384r1 | Subject: odc.officeapps.live.com
SNI: secp256r1 | Subject: services.gfe.nvidia.com
```

```
SNI: secp256r1 | Subject: services.gfe.nvidia.com
SNI: secp384r1 | Subject: officeclient.microsoft.com
SNI: x25519 | Subject: g.live.com
SNI: secp384r1 | Subject: odc.officeapps.live.com
SNI: secp256r1 | Subject: oneclient.sfx.ms
SNI: secp384r1 | Subject:
geo.prod.do.dsp.mp.microsoft.com
🔑 SNI: secp256r1 | Subject:
kv801.prod.do.dsp.mp.microsoft.com
SNI: secp256r1 | Subject:
cp801.prod.do.dsp.mp.microsoft.com
```

```
SNI: secp256r1 | Subject:
cp801.prod.do.dsp.mp.microsoft.com
SNI: secp256r1 | Subject:
disc801.prod.do.dsp.mp.microsoft.com
🔑 SNI: secp256r1 | Subject:
disc801.prod.do.dsp.mp.microsoft.com
SNI: secp256r1 | Subject:
disc801.prod.do.dsp.mp.microsoft.com
```

```
SNI: secp256r1 | Subject:
disc801.prod.do.dsp.mp.microsoft.com
SNI: secp256r1 | Subject:
disc801.prod.do.dsp.mp.microsoft.com
SNI: secp384r1 | Subject:
array804.prod.do.dsp.mp.microsoft.com
SNI: secp384r1 | Subject:
array805.prod.do.dsp.mp.microsoft.com
SNI: secp384r1 | Subject:
array803.prod.do.dsp.mp.microsoft.com
SNI: secp384r1 | Subject:
array804.prod.do.dsp.mp.microsoft.com
🔑 SNI: secp384r1 | Subject:
array805.prod.do.dsp.mp.microsoft.com
SNI: secp384r1 | Subject:
array816.prod.do.dsp.mp.microsoft.com
🔑 SNI: secp384r1 | Subject:
array804.prod.do.dsp.mp.microsoft.com
SNI: secp384r1 | Subject:
array807.prod.do.dsp.mp.microsoft.com
```

```
SNI: secp256r1 | Subject:
kv801.prod.do.dsp.mp.microsoft.com
🔑 SNI: secp256r1 | Subject:
kv801.prod.do.dsp.mp.microsoft.com
SNI: secp384r1 | Subject: login.microsoftonline.com
SNI: secp384r1 | Subject: fd.api.iris.microsoft.com
SNI: secp384r1 | Subject: login.microsoftonline.com
```

```
SNI: secp384r1 | Subject: settings-win.data.microsoft.com
SNI: secp384r1 | Subject: windows.msn.com
SNI: secp384r1 | Subject: windows.msn.com
SNI: secp384r1 | Subject: www.msn.com
SNI: secp384r1 | Subject: www.msn.com
SNI: x25519 | Subject: assets.msn.com
SNI: secp384r1 | Subject: api.msn.com
SNI: secp384r1 | Subject: srtb.msn.com
SNI: x25519 | Subject: img-s-msn-com.akamaized.net
SNI: secp384r1 | Subject: v10.events.data.microsoft.com
SNI: secp384r1 | Subject: v20.events.data.microsoft.com
SNI: - | Subject: 45.125.66.32
SNI: unknown-4588 | Subject: clients2.google.com
SNI: secp256r1 | Subject: static.edge.microsoftapp.net
```

```
SNI: secp384r1 | Subject: config.edge.skype.com
SNI: secp384r1 | Subject: edge.microsoft.com
SNI: secp384r1 | Subject: login.microsoftonline.com
SNI: secp384r1 | Subject: config.edge.skype.com
SNI: unknown-4588 | Subject: clients2.google.com
SNI: secp384r1 | Subject: edge.microsoft.com
SNI: - | Subject: 45.125.66.32
SNI: secp256r1 | Subject: static.edge.microsoftapp.net
🔑 SNI: unknown-4588 | Subject:
clients2.googleusercontent.com
SNI: - | Subject: 45.125.66.32
🔑 SNI: - | Subject: -
SNI: secp384r1 | Subject: login.microsoftonline.com
🔑 SNI: secp256r1 | Subject:
prod.client.wosc.services.microsoft.com
```

```
SNI: secp384r1 | Subject: login.live.com
SNI: secp384r1 | Subject: settings-win.data.microsoft.com
SNI: secp384r1 | Subject: fe2cr.update.microsoft.com
🔑 SNI: secp256r1 | Subject:
cp801.prod.do.dsp.mp.microsoft.com
SNI: secp256r1 | Subject:
geover.prod.do.dsp.mp.microsoft.com
🔑 SNI: secp256r1 | Subject:
kv801.prod.do.dsp.mp.microsoft.com
SNI: secp384r1 | Subject: v10.events.data.microsoft.com
SNI: secp384r1 | Subject: v10.events.data.microsoft.com
SNI: secp384r1 | Subject: v10.events.data.microsoft.com
SNI: secp384r1 | Subject: login.microsoftonline.com
SNI: secp384r1 | Subject: login.microsoftonline.com
SNI: secp384r1 | Subject: windows.msn.com
SNI: secp384r1 | Subject: v20.events.data.microsoft.com
```

```
SNI: secp384r1 | Subject: v10.events.data.microsoft.com
SNI: secp384r1 | Subject:
array807.prod.do.dsp.mp.microsoft.com
🔑 SNI: secp256r1 | Subject:
kv801.prod.do.dsp.mp.microsoft.com
🔑 SNI: secp384r1 | Subject:
mobile.events.data.microsoft.com
SNI: secp384r1 | Subject: login.microsoftonline.com
SNI: - | Subject: 45.125.66.32
SNI: unknown-4588 | Subject: clients2.google.com
SNI: secp256r1 | Subject: static.edge.microsoftapp.net
SNI: secp384r1 | Subject: config.edge.skype.com
SNI: secp384r1 | Subject: edge.microsoft.com
SNI: secp384r1 | Subject: login.microsoftonline.com
SNI: unknown-4588 | Subject: clients2.google.com
SNI: secp256r1 | Subject: static.edge.microsoftapp.net
```

```
SNI: secp384r1 | Subject: config.edge.skype.com
SNI: secp384r1 | Subject: edge.microsoft.com
SNI: secp384r1 | Subject: login.microsoftonline.com
SNI: unknown-4588 | Subject:
clients2.googleusercontent.com
SNI: - | Subject: 45.125.66.32
SNI: secp256r1 | Subject: edge-mobile-
static.azureedge.net
SNI: - | Subject: 45.125.66.32
SNI: - | Subject: -
SNI: - | Subject: 45.125.66.32
SNI: x25519 | Subject: g.live.com
SNI: secp256r1 | Subject: oneclient.sfx.ms
SNI: secp256r1 | Subject: static.edge.microsoftapp.net
SNI: unknown-4588 | Subject: clients2.google.com
```

```
SNI: secp384r1 | Subject: config.edge.skype.com
SNI: secp384r1 | Subject: edge.microsoft.com
SNI: secp384r1 | Subject: login.microsoftonline.com
SNI: unknown-4588 | Subject: clients2.google.com
SNI: secp256r1 | Subject: static.edge.microsoftapp.net
SNI: secp384r1 | Subject: config.edge.skype.com
SNI: secp384r1 | Subject: edge.microsoft.com
SNI: secp384r1 | Subject: login.microsoftonline.com
SNI: - | Subject: 45.125.66.32
SNI: unknown-4588 | Subject:
clients2.googleusercontent.com
SNI: - | Subject: 45.125.66.32
🔑 SNI: - | Subject: -
SNI: x25519 | Subject: g.live.com
```

```
SNI: secp256r1 | Subject: oneclient.sfx.ms
SNI: secp384r1 | Subject: ecs.office.com
SNI: secp256r1 | Subject:
prod.client.wosc.services.microsoft.com
SNI: secp384r1 | Subject: login.microsoftonline.com
SNI: secp384r1 | Subject: settings-win.data.microsoft.com
SNI: secp384r1 | Subject: settings-win.data.microsoft.com
SNI: secp384r1 | Subject:
array804.prod.do.dsp.mp.microsoft.com
SNI: secp256r1 | Subject:
kv801.prod.do.dsp.mp.microsoft.com
SNI: secp384r1 | Subject: ecs.office.com
SNI: secp384r1 | Subject: ecs.office.com
```

TLS Sessions (Suricata)

SNI: odc.officeapps.live.com | Subject: C=US, ST=WA,
L=Redmond, O=Microsoft Corporation,
CN=odc.officeapps.live.com

```
🔑 SNI: services.gfe.nvidia.com | Subject: C=US,
ST=California, L=Santa Clara, O=NVIDIA Corporation,
CN=it.nvidia.com
SNI: v10.events.data.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=WSE,
CN=*.events.data.microsoft.com
🔑 SNI: kv801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801-
prod.do.dsp.mp.microsoft.com
SNI: client.wns.windows.com | Subject: C=US, ST=WA,
L=Redmond, O=Microsoft Corporation, CN=*.wns.windows.com
SNI: geo.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft, OU=DSP,
CN=*.prod.do.dsp.mp.microsoft.com
SNI: browser.events.data.msn.com | Subject: None
SNI: windows.msn.com | Subject: None
SNI: r.bing.com | Subject: None
SNI: officeclient.microsoft.com | Subject: C=US, ST=WA,
L=Redmond, O=Microsoft Corporation,
CN=config.officeapps.live.com
SNI: ntp.msn.com | Subject: None
```

```
SNI: www.msn.com | Subject: None
SNI: odc.officeapps.live.com | Subject: C=US, ST=WA,
L=Redmond, O=Microsoft Corporation,
CN=odc.officeapps.live.com
SNI: www.bing.com | Subject: None
SNI: www.bing.com | Subject: None
SNI: oneclient.sfx.ms | Subject: C=US, ST=WA, L=Redmond,
O=Microsoft Corporation, CN=*.sfx.ms
SNI: v20.events.data.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=WSE,
CN=*.events.data.microsoft.com
SNI: assets.msn.com | Subject: None
SNI: g.live.com | Subject: C=US, ST=WA, L=Redmond,
O=Microsoft Corporation, CN=q.msn.com
SNI: static.edge.microsoftapp.net | Subject: None
🔑 SNI: google-authenticator.burleson-appliance.net |
Subject: None
SNI: services.gfe.nvidia.com | Subject: C=US,
ST=California, L=Santa Clara, O=NVIDIA Corporation,
CN=it.nvidia.com
```

```
SNI: azure.microsoft.com | Subject: None
SNI: assets.msn.com | Subject: None
SNI: login.microsoftonline.com | Subject: None
SNI: appointedtimeagriculture.com | Subject: None
SNI: edge.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft Corporation,
CN=edge.microsoft.com
SNI: browser.events.data.msn.com | Subject: None
SNI: www.bing.com | Subject: None
SNI: www.bing.com | Subject: None
SNI: www.microsoft.com | Subject: None
SNI: c.msn.com | Subject: C=US, ST=WA, L=Redmond,
O=Microsoft Corporation, CN=c.msn.com
SNI: edge.microsoft.com | Subject: None
SNI: www.microsoft.com | Subject: None
SNI: edge.microsoft.com | Subject: None
```

```
SNI: lpcdn.lpsnmedia.net | Subject: None
SNI: publisher.liveperson.net | Subject: None
SNI: browser.events.data.msn.com | Subject: None
SNI: browser.events.data.microsoft.com | Subject: None
SNI: dpm.demdex.net | Subject: None
SNI: authenticatoor.org | Subject: None
SNI: azure.microsoft.com | Subject: None
SNI: edge.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft Corporation,
CN=edge.microsoft.com
SNI: js.monitor.azure.com | Subject: None
SNI: login.microsoftonline.com | Subject: None
SNI: checkappexec.microsoft.com | Subject: None
SNI: azure.microsoft.com | Subject: None
SNI: azure.microsoft.com | Subject: None
```

```
SNI: googleads.g.doubleclick.net | Subject: None
SNI: ds.reson8.com | Subject: None
SNI: edge-consumer-static.azureedge.net | Subject: None
SNI: va.v.liveperson.net | Subject: C=US, ST=New York,
O=LivePerson, Inc, CN=*.v.liveperson.net
SNI: i.clarity.ms | Subject: C=US, ST=WA, L=Redmond,
O=Microsoft Corporation, CN=a.clarity.ms
SNI: assets.msn.com | Subject: None
SNI: px.owneriq.net | Subject: C=US, ST=North Carolina,
L=Winston-Salem, O=Inmar Inc, CN=*.owneriq.net
SNI: play.vidyard.com | Subject: CN=*.vidyard.com
SNI: px.owneriq.net | Subject: None
SNI: www.clarity.ms | Subject: None
SNI: ag.innovid.com | Subject: CN=*.innovid.com
SNI: accdn.lpsnmedia.net | Subject: C=US, ST=New York,
O=LivePerson, Inc, CN=*.lpsnmedia.net
```

```
SNI: c.go-mpulse.net | Subject: None
SNI: cdn-dynmedia-1.microsoft.com | Subject: None
SNI: azure.microsoft.com | Subject: None
SNI: lptag.liveperson.net | Subject: C=US, ST=New York,
O=LivePerson, Inc, CN=*.liveperson.net
SNI: azure.microsoft.com | Subject: None
SNI: assets.adobedtm.com | Subject: None
SNI: dc.ads.linkedin.com | Subject: C=US, ST=California,
L=Sunnyvale, O=LinkedIn Corporation, CN=www.linkedin.com
SNI: c1.microsoft.com | Subject: C=US, ST=WA, L=Redmond,
O=Microsoft Corporation, CN=c.msn.com
SNI: dmpsync.3lift.com | Subject: None
SNI: browser.events.data.microsoft.com | Subject: None
SNI: c.bing.com | Subject: None
SNI: mscom.demdex.net | Subject: None
SNI: bat.bing.com | Subject: None
```

```
SNI: www.facebook.com | Subject: None
SNI: windows.msn.com | Subject: None
SNI: api.msn.com | Subject: None
SNI: jadserve.postrelease.com | Subject:
CN=*.postrelease.com
SNI: img-s-msn-com.akamaized.net | Subject: None
SNI: www.google.com | Subject: None
SNI: cms.analytics.yahoo.com | Subject: None
SNI: bttrack.com | Subject: CN=*.bttrack.com
SNI: login.microsoftonline.com | Subject: None
SNI: settings-win.data.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft, OU=WSE, CN=settings-
win.data.microsoft.com
SNI: www.bing.com | Subject: None
SNI: windows.msn.com | Subject: None
SNI: www.msn.com | Subject: None
```

SNI: login.microsoftonline.com | Subject: None

SNI: edge.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft Corporation,
CN=edge.microsoft.com

SNI: login.microsoftonline.com | Subject: None

SNI: fd.api.iris.microsoft.com | Subject: C=US, ST=WA,
L=Redmond, O=Microsoft Corporation, CN=arc.msn.com

SNI: v20.events.data.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=WSE,
CN=*.events.data.microsoft.com

SNI: array804.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=DSP,
CN=*.prod.do.dsp.mp.microsoft.com

SNI: odc.officeapps.live.com | Subject: C=US, ST=WA,
L=Redmond, O=Microsoft Corporation,
CN=odc.officeapps.live.com

SNI: kv801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: services.gfe.nvidia.com | Subject: C=US,
ST=California, L=Santa Clara, O=NVIDIA Corporation,
CN=it.nvidia.com

SNI: officeclient.microsoft.com | Subject: C=US, ST=WA,
L=Redmond, O=Microsoft Corporation,
CN=config.officeapps.live.com

SNI: odc.officeapps.live.com | Subject: C=US, ST=WA,
L=Redmond, O=Microsoft Corporation,
CN=odc.officeapps.live.com

SNI: oneclient.sfx.ms | Subject: C=US, ST=WA, L=Redmond,
0=Microsoft Corporation, CN=*.sfx.ms

SNI: g.live.com | Subject: C=US, ST=WA, L=Redmond,
0=Microsoft Corporation, CN=g.msn.com

SNI: officeclient.microsoft.com | Subject: C=US, ST=WA,
L=Redmond, O=Microsoft Corporation,
CN=config.officeapps.live.com

SNI: kv801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: array803.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=DSP,
CN=*.prod.do.dsp.mp.microsoft.com

SNI: cp801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: services.gfe.nvidia.com | Subject: C=US,
ST=California, L=Santa Clara, O=NVIDIA Corporation,
CN=it.nvidia.com

SNI: disc801.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft Corporation,
CN=cp801-prod.do.dsp.mp.microsoft.com

SNI: www.msn.com | Subject: None

SNI: cp801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: disc801.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft Corporation,
CN=cp801-prod.do.dsp.mp.microsoft.com

SNI: cp801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: array816.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=DSP,
CN=*.prod.do.dsp.mp.microsoft.com

SNI: srtb.msn.com | Subject: None

SNI: cp801.prod.do.dsp.mp.microsoft.com | Subject: C=US, ST=WA, L=Redmond, 0=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: array804.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, 0=Microsoft, 0U=DSP,
CN=*.prod.do.dsp.mp.microsoft.com

SNI: cp801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: login.microsoftonline.com | Subject: None

SNI: kv801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: disc801.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft Corporation,
CN=cp801-prod.do.dsp.mp.microsoft.com

SNI: windows.msn.com | Subject: None

SNI: v10.events.data.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=WSE,
CN=*.events.data.microsoft.com

SNI: disc801.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft Corporation,
CN=cp801-prod.do.dsp.mp.microsoft.com

SNI: 45.125.66.32 | Subject: C=XX, ST=N/A, L=N/A, 0=Selfsigned certificate, CN=45.125.66.32: Self-signed
certificate

SNI: array804.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, 0=Microsoft, 0U=DSP,
CN=*.prod.do.dsp.mp.microsoft.com

SNI: cp801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, 0=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: kv801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: cp801.prod.do.dsp.mp.microsoft.com | Subject: C=US, ST=WA, L=Redmond, 0=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: kv801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, 0=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: disc801.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft Corporation,
CN=cp801-prod.do.dsp.mp.microsoft.com

SNI: kv801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: array805.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=DSP,
CN=*.prod.do.dsp.mp.microsoft.com

SNI: kv801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: kv801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, 0=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: kv801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: login.microsoftonline.com | Subject: None

SNI: cp801.prod.do.dsp.mp.microsoft.com | Subject: C=US, ST=WA, L=Redmond, 0=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: static.edge.microsoftapp.net | Subject: None

SNI: disc801.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, 0=Microsoft Corporation,
CN=cp801-prod.do.dsp.mp.microsoft.com

SNI: array804.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=DSP,
CN=*.prod.do.dsp.mp.microsoft.com

SNI: array805.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=DSP,
CN=*.prod.do.dsp.mp.microsoft.com

SNI: login.microsoftonline.com | Subject: None

SNI: array807.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=DSP,
CN=*.prod.do.dsp.mp.microsoft.com

SNI: kv801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: edge.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft Corporation,
CN=edge.microsoft.com

SNI: edge.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft Corporation,
CN=edge.microsoft.com

SNI: clients2.google.com | Subject: None

SNI: fd.api.iris.microsoft.com | Subject: C=US, ST=WA,
L=Redmond, O=Microsoft Corporation, CN=arc.msn.com

SNI: None | Subject: C=XX, ST=N/A, L=N/A, 0=Self-signed certificate, CN=45.125.66.252: Self-signed certificate

SNI: settings-win.data.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft, OU=WSE, CN=settingswin.data.microsoft.com

SNI: fe2cr.update.microsoft.com | Subject: C=US, ST=WA,
L=Redmond, O=Microsoft, OU=DSP,
CN=fe2cr.update.microsoft.com

```
SNI: login.microsoftonline.com | Subject: None
SNI: geover.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp501-
prod.do.dsp.mp.microsoft.com
SNI: settings-win.data.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft, OU=WSE, CN=settings-
win.data.microsoft.com
SNI: login.microsoftonline.com | Subject: None
SNI: v20.events.data.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=WSE,
CN=*.events.data.microsoft.com
SNI: static.edge.microsoftapp.net | Subject: None
SNI: 45.125.66.32 | Subject: C=XX, ST=N/A, L=N/A, 0=Self-
signed certificate, CN=45.125.66.32: Self-signed
certificate
SNI: v10.events.data.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=WSE,
CN=*.events.data.microsoft.com
SNI: windows.msn.com | Subject: None
SNI: 45.125.66.32 | Subject: C=XX, ST=N/A, L=N/A, 0=Self-
```

signed certificate, CN=45.125.66.32: Self-signed

certificate

```
SNI: api.msn.com | Subject: None
SNI: srtb.msn.com | Subject: None
SNI: mobile.events.data.microsoft.com | Subject: None
SNI: www.msn.com | Subject: None
SNI: assets.msn.com | Subject: None
SNI: img-s-msn-com.akamaized.net | Subject: None
SNI: edge-mobile-static.azureedge.net | Subject: None
SNI: 45.125.66.32 | Subject: C=XX, ST=N/A, L=N/A, 0=Self-
signed certificate, CN=45.125.66.32: Self-signed
certificate
SNI: 45.125.66.32 | Subject: C=XX, ST=N/A, L=N/A, 0=Self-
signed certificate, CN=45.125.66.32: Self-signed
certificate
SNI: kv801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801-
prod.do.dsp.mp.microsoft.com
SNI: th.bing.com | Subject: None
```

```
SNI: None | Subject: C=XX, ST=N/A, L=N/A, 0=Self-signed
certificate, CN=45.125.66.252: Self-signed certificate
SNI: v10.events.data.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=WSE,
CN=*.events.data.microsoft.com
SNI: windows.msn.com | Subject: None
SNI: kv801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801-
prod.do.dsp.mp.microsoft.com
SNI: login.microsoftonline.com | Subject: None
SNI: static.edge.microsoftapp.net | Subject: None
SNI: clients2.google.com | Subject: None
SNI: login.microsoftonline.com | Subject: None
SNI: edge.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft Corporation,
CN=edge.microsoft.com
SNI: clients2.google.com | Subject: None
SNI: config.edge.skype.com | Subject: None
```

```
SNI: 45.125.66.32 | Subject: C=XX, ST=N/A, L=N/A, 0=Self-
signed certificate, CN=45.125.66.32: Self-signed
certificate
```

SNI: login.microsoftonline.com | Subject: None

SNI: 45.125.66.32 | Subject: C=XX, ST=N/A, L=N/A, 0=Selfsigned certificate, CN=45.125.66.32: Self-signed
certificate

SNI: edge.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft Corporation,
CN=edge.microsoft.com

SNI: 45.125.66.32 | Subject: C=XX, ST=N/A, L=N/A, 0=Selfsigned certificate, CN=45.125.66.32: Self-signed
certificate

SNI: ecs.office.com | Subject: None

SNI: None | Subject: C=XX, ST=N/A, L=N/A, O=Self-signed
certificate, CN=45.125.66.252: Self-signed certificate

SNI: array804.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=DSP,
CN=*.prod.do.dsp.mp.microsoft.com

SNI: static.edge.microsoftapp.net | Subject: None

SNI: www.bing.com | Subject: None

```
SNI: ecs.office.com | Subject: None
SNI: g.live.com | Subject: C=US, ST=WA, L=Redmond,
O=Microsoft Corporation, CN=g.msn.com
SNI: clients2.google.com | Subject: None
SNI: array807.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=DSP,
CN=*.prod.do.dsp.mp.microsoft.com
SNI: login.microsoftonline.com | Subject: None
SNI: config.edge.skype.com | Subject: None
SNI: edge.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft Corporation,
CN=edge.microsoft.com
SNI: clients2.googleusercontent.com | Subject: None
SNI: prod.client.wosc.services.microsoft.com | Subject:
None
SNI: config.edge.skype.com | Subject: None
SNI: client.wns.windows.com | Subject: C=US, ST=WA,
L=Redmond, O=Microsoft Corporation, CN=*.wns.windows.com
```

```
SNI: prod.client.wosc.services.microsoft.com | Subject:
None
SNI: geo.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft, OU=DSP,
CN=*.prod.do.dsp.mp.microsoft.com
SNI: disc801.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft Corporation,
CN=cp801-prod.do.dsp.mp.microsoft.com
SNI: disc801.prod.do.dsp.mp.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft Corporation,
CN=cp801-prod.do.dsp.mp.microsoft.com
SNI: oneclient.sfx.ms | Subject: C=US, ST=WA, L=Redmond,
O=Microsoft Corporation, CN=*.sfx.ms
SNI: clients2.google.com | Subject: None
SNI: login.microsoftonline.com | Subject: None
SNI: static.edge.microsoftapp.net | Subject: None
SNI: config.edge.skype.com | Subject: None
SNI: ecs.office.com | Subject: None
SNI: kv801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801-
prod.do.dsp.mp.microsoft.com
```

```
SNI: v20.events.data.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=WSE,
CN=*.events.data.microsoft.com
```

SNI: cp801.prod.do.dsp.mp.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft Corporation, CN=cp801prod.do.dsp.mp.microsoft.com

SNI: v10.events.data.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=WSE,
CN=*.events.data.microsoft.com

SNI: v10.events.data.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft, OU=WSE,
CN=*.events.data.microsoft.com

SNI: config.edge.skype.com | Subject: None

SNI: login.live.com | Subject: C=US, ST=Washington,
L=Redmond, O=Microsoft Corporation, CN=login.live.com

SNI: edge.microsoft.com | Subject:
C=US, ST=WA, L=Redmond, O=Microsoft Corporation,
CN=edge.microsoft.com

SNI: static.edge.microsoftapp.net | Subject: None

SNI: clients2.google.com | Subject: None

SNI: 45.125.66.32 | Subject: C=XX, ST=N/A, L=N/A, 0=Selfsigned certificate, CN=45.125.66.32: Self-signed
certificate

```
SNI: g.live.com | Subject: C=US, ST=WA, L=Redmond,
O=Microsoft Corporation, CN=q.msn.com
SNI: settings-win.data.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft, OU=WSE, CN=settings-
win.data.microsoft.com
SNI: login.microsoftonline.com | Subject: None
SNI: config.edge.skype.com | Subject: None
SNI: oneclient.sfx.ms | Subject: C=US, ST=WA, L=Redmond,
O=Microsoft Corporation, CN=*.sfx.ms
SNI: login.microsoftonline.com | Subject: None
SNI: clients2.googleusercontent.com | Subject: None
🔑 SNI: settings-win.data.microsoft.com | Subject: C=US,
ST=WA, L=Redmond, O=Microsoft, OU=WSE, CN=settings-
win.data.microsoft.com
```

SNI: browser.events.data.msn.com | Subject: None

SNI: clients2.googleusercontent.com | Subject: None



No data found.

© Zeek Weird Events

```
? 10.1.17.2 | 10.1.17.215 → 58958
```

Kerberos Auth Logs

```
■ 10.1.17.215 → 10.1.17.2@88 | Success: TGS
■ 10.1.17.215 → 10.1.17.2@88 | Success: TGS
■ 10.1.17.215 → 10.1.17.2@88 | Success: AS
■ 10.1.17.215 → 10.1.17.2@88 | Success: AS
■ 10.1.17.215 → 10.1.17.2@88 | Success: TGS
■ 10.1.17.215 → 10.1.17.2@445 | Success: -
■ 10.1.17.215 → 10.1.17.2@88 | Success: TGS
```

```
■ 10.1.17.215 → 10.1.17.2@445 | Success: -
```

SMB Access Logs

No data found.

RDP Sessions

No data found.

Generated by BeezPCAP 🐝