2024
FIRST
Cyber Threat
Intelligence
Conference

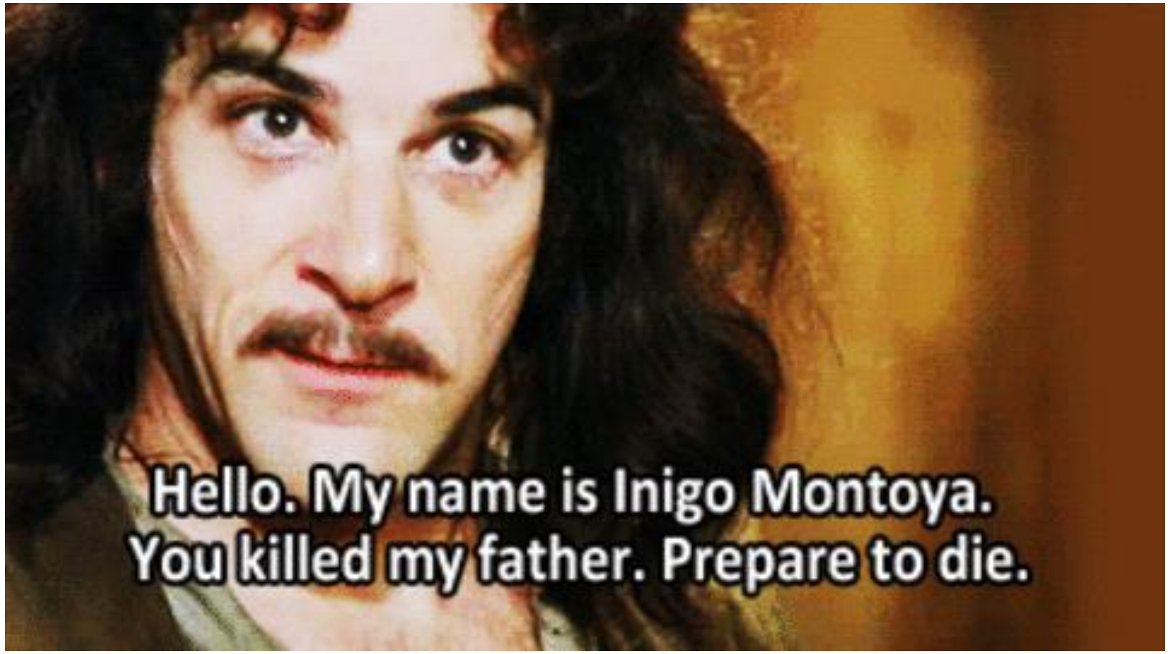
Berlin, Germany
April 15-17, 2024

Invisible Strings – Contemporary Challenges And Techniques Of Infrastructure Tracking

Kamil Bojarski

Berlin, 16.04.2024

whoami


Hello. My name is Inigo Montoya.
You killed my father. Prepare to die.

1. Greeting.
2. Introduce yourself.
3. Establish personal link.
4. Manage expectations.

Picture source: https://tenor.com/pl/view/inigo-montoya-hello-killed-my-father-gif-9985166

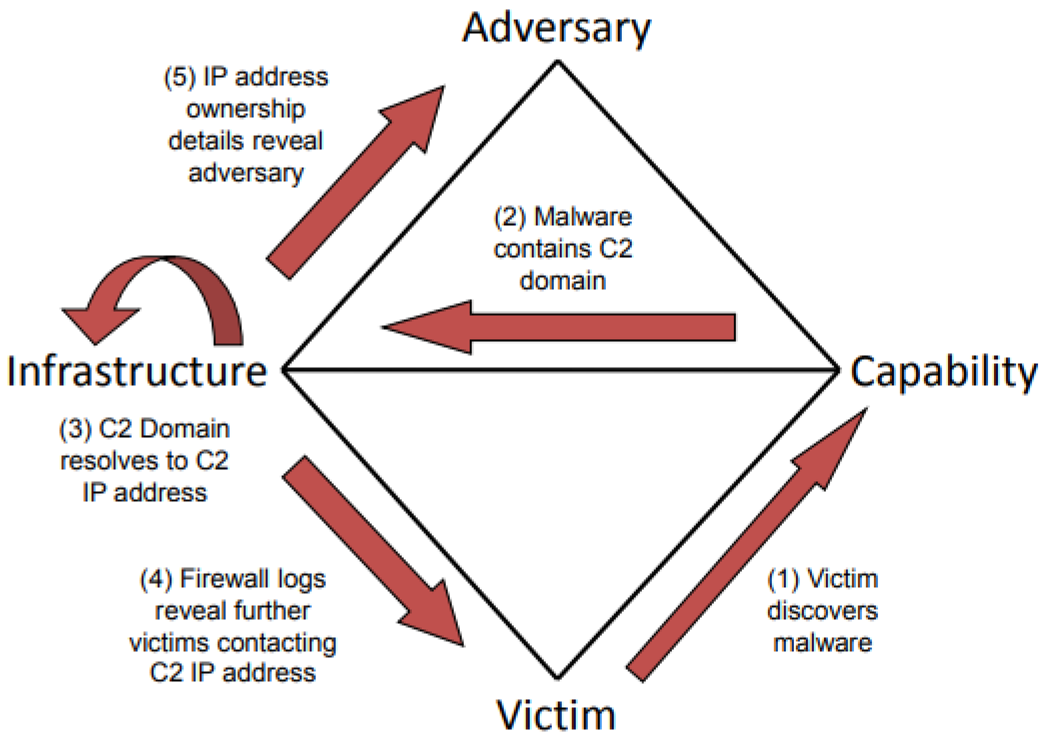
whoami

- Senior Analyst – Standard Chartered Client and Third-Party Intelligence team
- Teaching Assistant – SANS FOR578 Cyber Threat Intelligence
- European Cybersecurity Fellowship 2024-2025 Cohort
- You can read my thoughts on OSINT, national security, and threat intelligence at counterintelligence.pl
- Views, opinions, and conclusions presented here are my own and not of any of my current or past employers!

- Feel free to reach out:
  - kamil.bojarski@lawsec.net
  - @lawsecnet

Infrastructure Analysis in Threat Intelligence

- Allows tracking adversarial activities during recon and weaponization phases.
- Allows long term tracking of activity groups regardless of possibility to observe intrusions directly.
- Wealth of data avaialble from internet scanning services and indicator submission platforms.
- Main issues are related to signal to noise ration of findings.
- Let's cover methods, sources, and use cases of infrastructure tracking for defense operations.


Adversary
(5) IP address ownership details reveal adversary
(2) Malware contains C2 domain
Infrastructure
Capability
(3) C2 Domain resolves to C2 IP address
(4) Firewall logs reveal further victims contacting C2 IP address
(1) Victim discovers malware
Victim

Picture source: https://apps.dtic.mil/sti/pdfs/ADA586960.pdf

Infrastructure Tracking Along Kill-Chain

- Because of how internet facing adversarial assets are used, infrastructure hunting provides a unique opportunity to tackle earlier phases of kill-chain.
- One of the few opportunities to track weaponization.
- In terms of phishing attempts visibility into newly created infrastructure (victim branded credential harvesting panels) can provide early indicators of targeting.
- On the other end of the spectrum infrastructure insights can lead IR and compromise assessment efforts.
- Effective tracking of exfiltration nodes allow visibility into exfiltration.

Infrastructure Tracking Along Kill-Chain

Recon – hosts conducting mass scanning, direct network scanning attempts

Weaponization – tracking C2 nodes before use, phishing credential harvesting sites

Delivery – active phishing pages, second stage payload hosting

Command and Control – C2 communication, profiling active C2 nodes

Actions on Objective – data exfiltration, hands-on operations command input

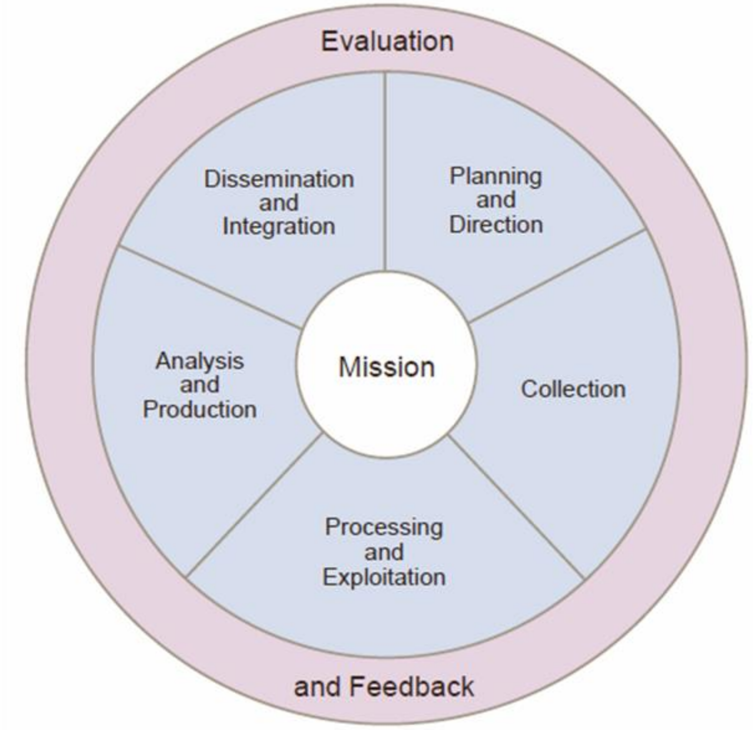
Applying Intelligence Cycle To Infrastructure Tracking

- As with every intelligence activity, correct intelligence requirements support proper direction of investigations and aligned outcomes.
- Multitude ways to approach the planning phase. From proactive detection of targeting of vendors to support for threat hunting and IR activities.
- Collection and processing will often involve working with data sets at scale.
- Outcomes will have operational implications, however can they can be also used to support strategic outlook.

Picture source: https://giphy.com/gifs/trust-the-process-jobs-not-finished-mPKa6OI5oRsmextwBq

Applying Intelligence Cycle To Infrastructure Tracking

- Planning and direction – proactive hunting for infrastructure created vs hunting for support of incident response and security operations.
- Collection – internet scanning sources, active vs passive collection, use of threat intelligence feeds.
- Processing – normalization of results from multiple sources, automatization of queries.
- Analysis – infrastructure profiling, pattern analysis, query building.
- Dissemination – indicator sharing, describing adversarial tradecraft.



Picture source: https://usnwc.libguides.com/c.php?g=494120&p=3381427

Applying Intelligence Cycle To Infrastructure Tracking

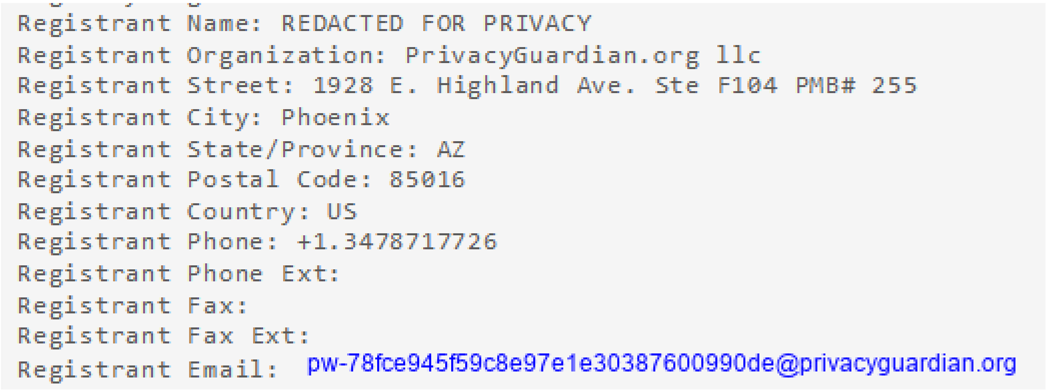
Tactical	Operational/Strategic
Discovery of related infrastucture during incident response.	Discovery of infrastructure based on external reporting.
Retrohunts based on temporal patterns of active infrastructure.	Establishing methodology of use and creation of infrastructure.
Early detection of phishing infrastructure.	Assessing use of infrastructure based on service configuration.
C2 node discovery and alerting or blocking.	

Breakdown of Sources

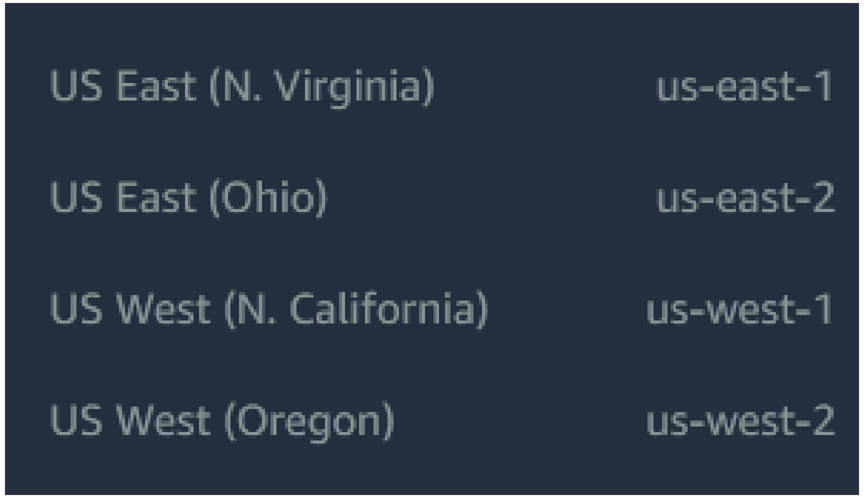
- Internet scanning services (general visibility):
  - Shodan
  - Censys
  - FOFA
  - GreyNoise
  - PassiveTotal (kinda :-( )
- File/URL submission services (already used assets):
  - VirusTotal
  - URLScan
  - Hybrid-Analysis
  - Intezer
- Threat intelligence exchange (analysis leads):
  - Pulsedive
  - Alienvault
  - Abuse.ch

Contemporary Challenges in Tracking

- C2 nodes have to be exposed for effective operations.
- But proliferation of public cloud services made quick rotation and setting up infra easy.
- Privacy protection for domain registration is very common.
- As such we can encounter very common profiles of infra that will not be useful for tracking or detection.
- This translates to high noise to signal ration that infrastructure hunters have to be aware of.



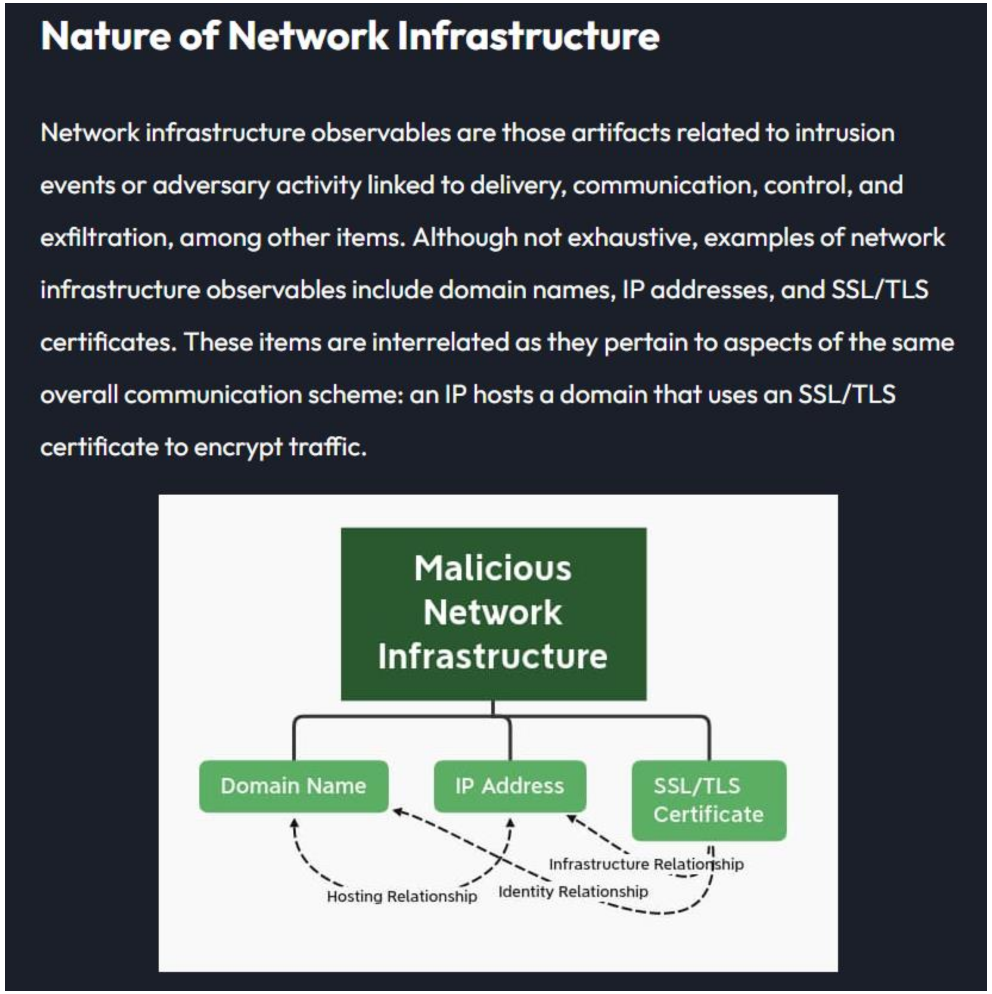
```
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: PrivacyGuardian.org llc
Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Registrant City: Phoenix
Registrant State/Province: AZ
Registrant Postal Code: 85016
Registrant Country: US
Registrant Phone: +1.3478717726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pw-78fce945f59c8e97e1e30387600990de@privacyguardian.org
```



US East (N. Virginia)	us-east-1
US East (Ohio)	us-east-2
US West (N. California)	us-west-1
US West (Oregon)	us-west-2

Infrastructure Indicators as Composite Objects

- Due to ease of creating infrastructure that blends in with legitimate assets, use of a single feature for resilient tracking is not viable.
- Combining multiple features into profiles allows switching from atomic indicator to TTP context.
- Contributes to both detection and understanding of the scope of adversarial activities and evolution over time
- Joe Slowik did a great job describing this approach in 2020.



Nature of Network Infrastructure

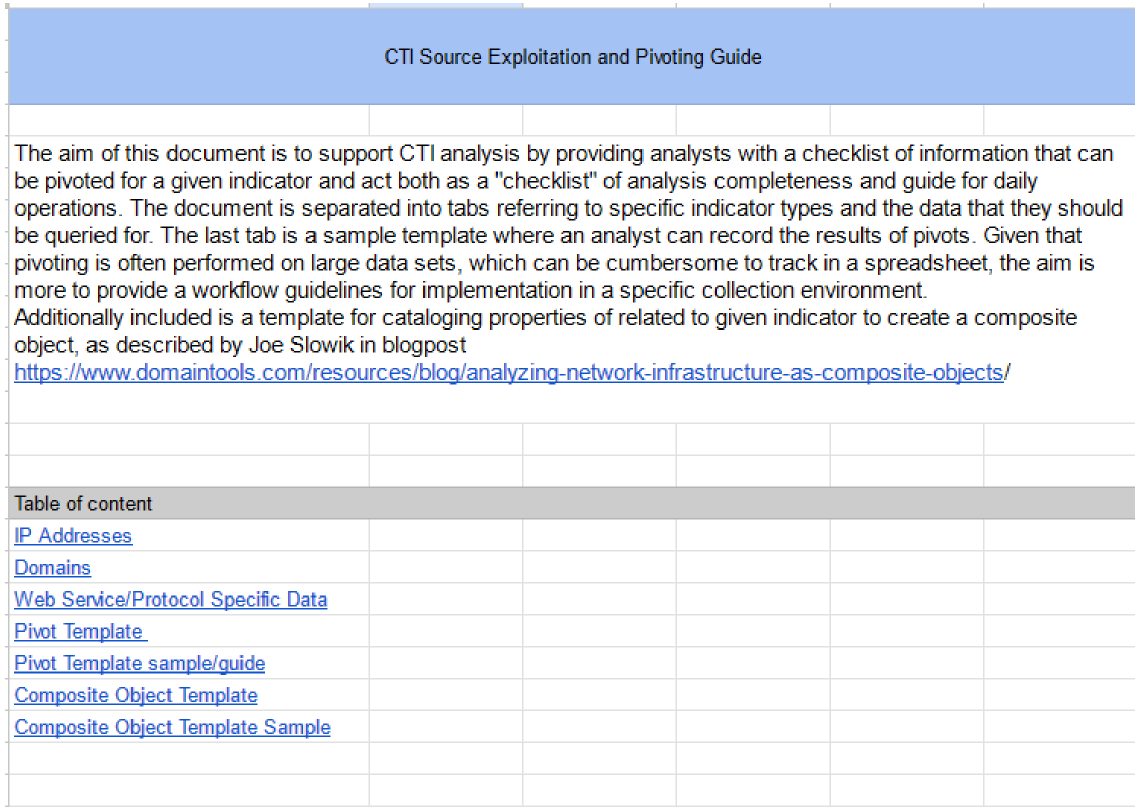
Network infrastructure observables are those artifacts related to intrusion events or adversary activity linked to delivery, communication, control, and exfiltration, among other items. Although not exhaustive, examples of network infrastructure observables include domain names, IP addresses, and SSL/TLS certificates. These items are interrelated as they pertain to aspects of the same overall communication scheme: an IP hosts a domain that uses an SSL/TLS certificate to encrypt traffic.

Picture source: https://www.domaintools.com/resources/blog/analyzing-network-infrastructure-as-composite-objects/

Picture source: https://imageresizer.com/meme-generator/edit/angry-penguin

Profiling Infrastructure Creation

- To move from atomic observables, we need to understand how the threat actor approach setting up infrastructure.
- As with all instances of TTPs this is not convenient for a TA to change.
- Especially true for eCrime activities where actors are more interested in scaling activity to a large number of victims rather than conducting targeted intrusions.
- bit.ly/infrastructure-exploitation



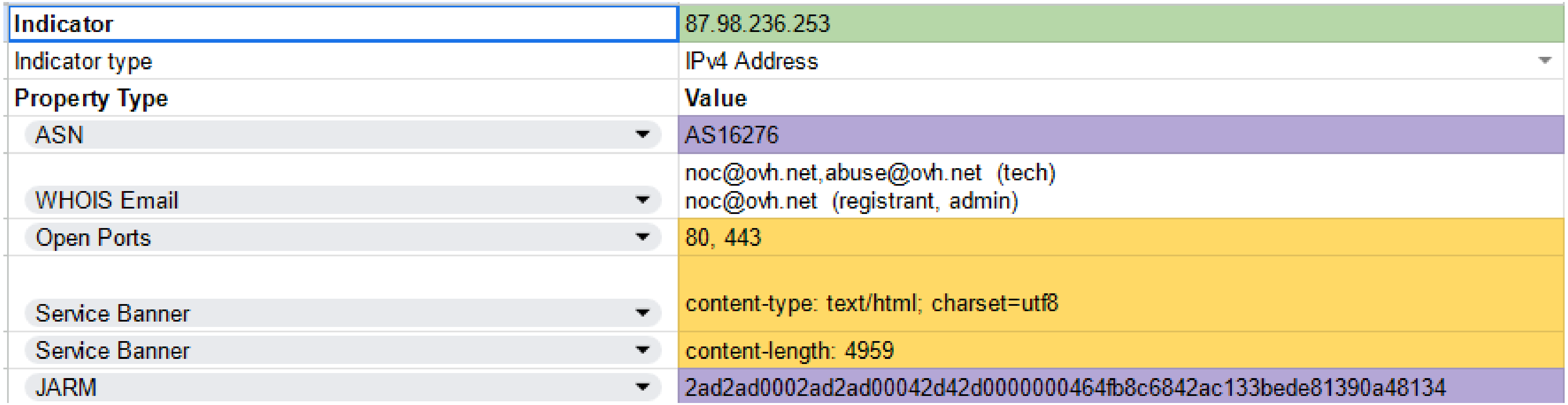
CTI Source Exploitation and Pivoting Guide

The aim of this document is to support CTI analysis by providing analysts with a checklist of information that can be pivoted for a given indicator and act both as a "checklist" of analysis completeness and guide for daily operations. The document is separated into tabs referring to specific indicator types and the data that they should be queried for. The last tab is a sample template where an analyst can record the results of pivots. Given that pivoting is often performed on large data sets, which can be cumbersome to track in a spreadsheet, the aim is more to provide a workflow guidelines for implementation in a specific collection environment.
Additionally included is a template for cataloging properties of related to given indicator to create a composite object, as described by Joe Slowik in blogpost
https://www.domaintools.com/resources/blog/analyzing-network-infrastructure-as-composite-objects/

Table of content

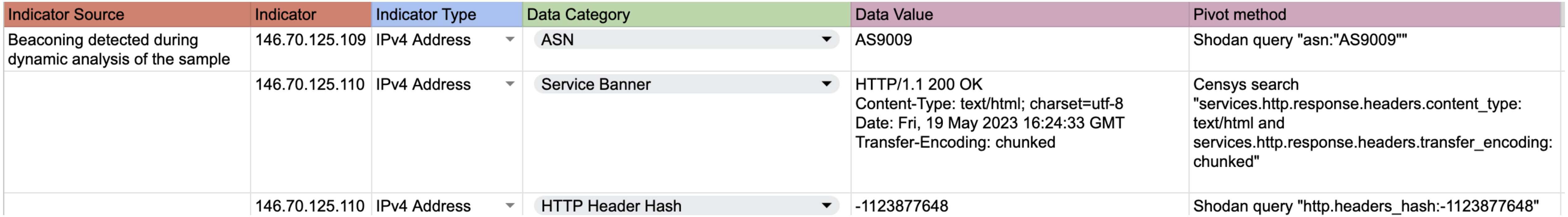
IP Addresses
Domains
Web Service/Protocol Specific Data
Pivot Template
Pivot Template sample/guide
Composite Object Template
Composite Object Template Sample

Profiling Infrastructure Creation



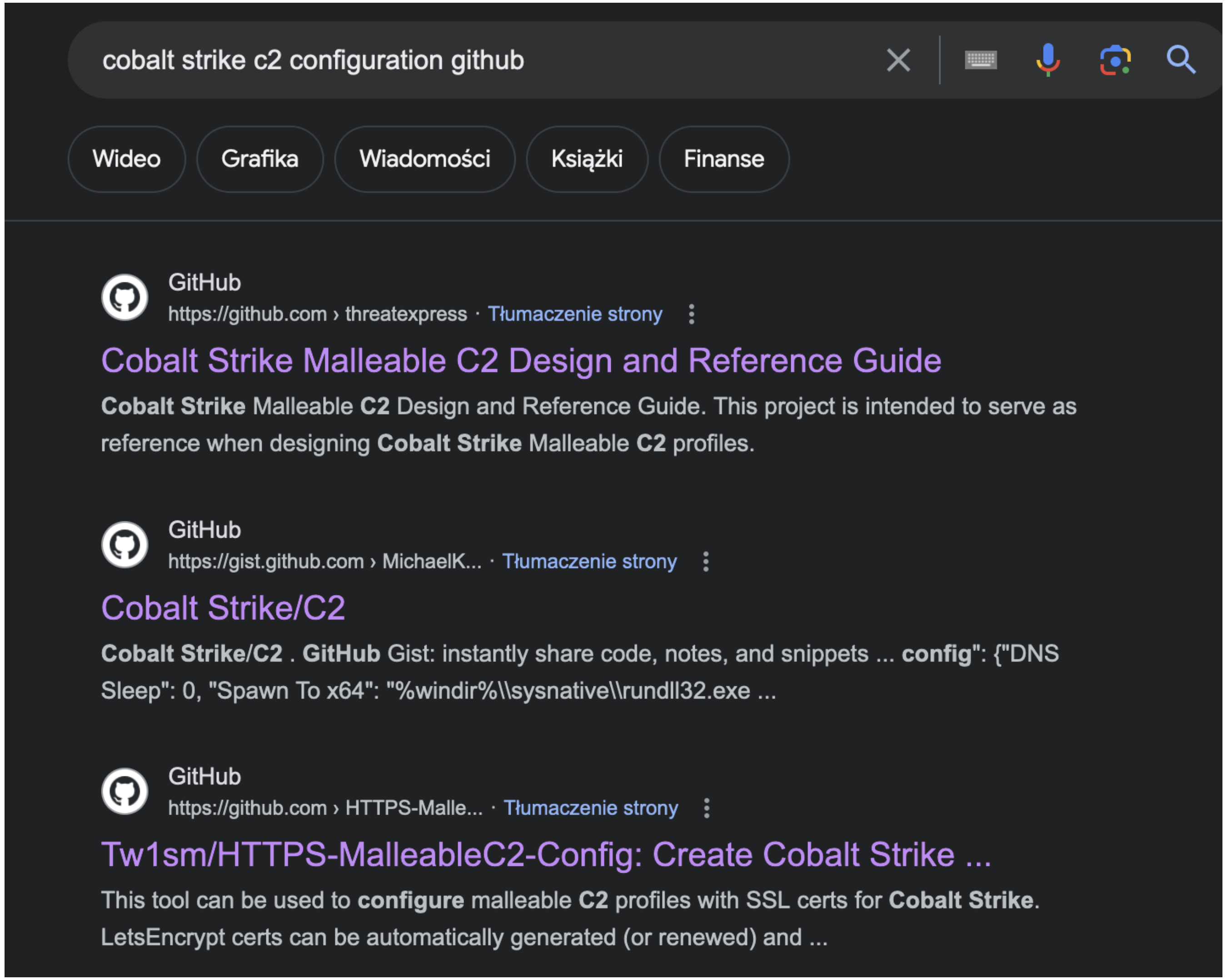
Indicator	87.98.236.253
Indicator type	IPv4 Address
Property Type	**Value**
ASN	AS16276
WHOIS Email	noc@ovh.net,abuse@ovh.net (tech) noc@ovh.net (registrant, admin)
Open Ports	80, 443
Service Banner	content-type: text/html; charset=utf8
Service Banner	content-length: 4959
JARM	2ad2ad0002ad2ad00042d42d0000000464fb8c6842ac133bede81390a48134

Profiling Infrastructure Creation



Indicator Source	Indicator	Indicator Type	Data Category	Data Value	Pivot method
Beaconing detected during dynamic analysis of the sample	146.70.125.109	IPv4 Address	ASN	AS9009	Shodan query "asn:"AS9009""
	146.70.125.110	IPv4 Address	Service Banner	HTTP/1.1 200 OK Content-Type: text/html; charset=utf-8 Date: Fri, 19 May 2023 16:24:33 GMT Transfer-Encoding: chunked	Censys search "services.http.response.headers.content_type: text/html and services.http.response.headers.transfer_encoding: chunked"
	146.70.125.110	IPv4 Address	HTTP Header Hash	-1123877648	Shodan query "http.headers_hash:-1123877648"

Cobalt Strike Malleable Profiles



GitHub
https://github.com › threatexpress · Tłumaczenie strony

Cobalt Strike Malleable C2 Design and Reference Guide

Cobalt Strike Malleable **C2** Design and Reference Guide. This project is intended to serve as reference when designing **Cobalt Strike** Malleable **C2** profiles.

GitHub
https://gist.github.com › MichaelK... · Tłumaczenie strony

Cobalt Strike/C2

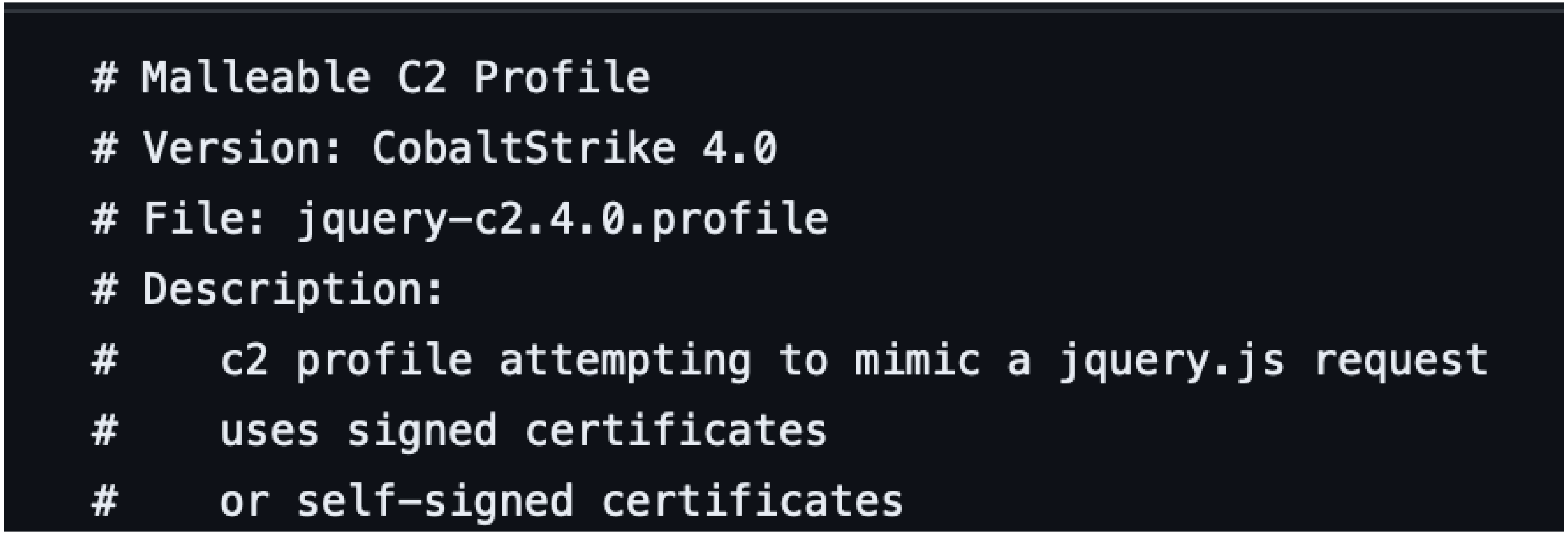
Cobalt Strike/C2 . **GitHub** Gist: instantly share code, notes, and snippets ... **config**": {"DNS Sleep": 0, "Spawn To x64": "%windir%\\sysnative\\rundll32.exe ...

GitHub
https://github.com › HTTPS-Malle... · Tłumaczenie strony

Tw1sm/HTTPS-MalleableC2-Config: Create Cobalt Strike ...

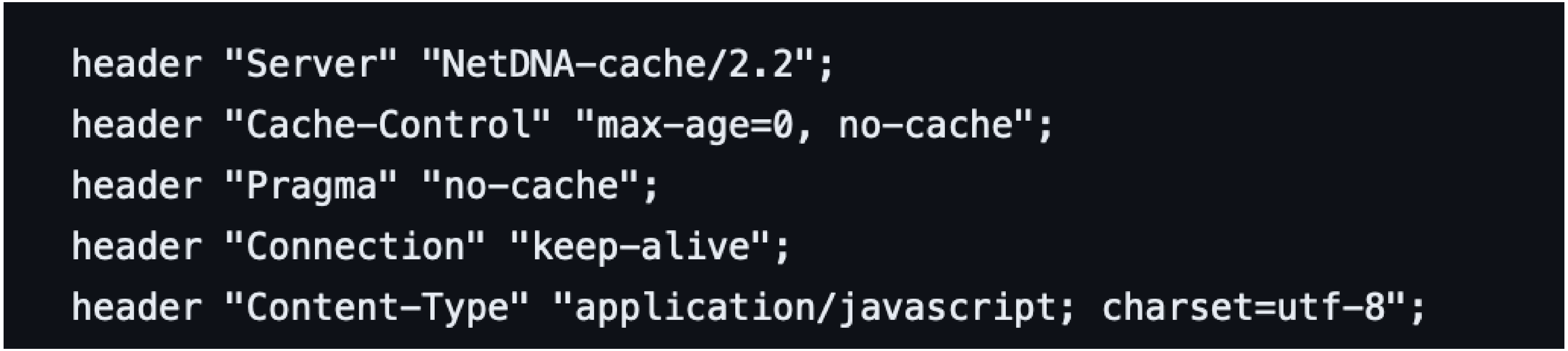
This tool can be used to **configure** malleable **C2** profiles with SSL certs for **Cobalt Strike**. LetsEncrypt certs can be automatically generated (or renewed) and ...

Cobalt Strike Malleable Profiles



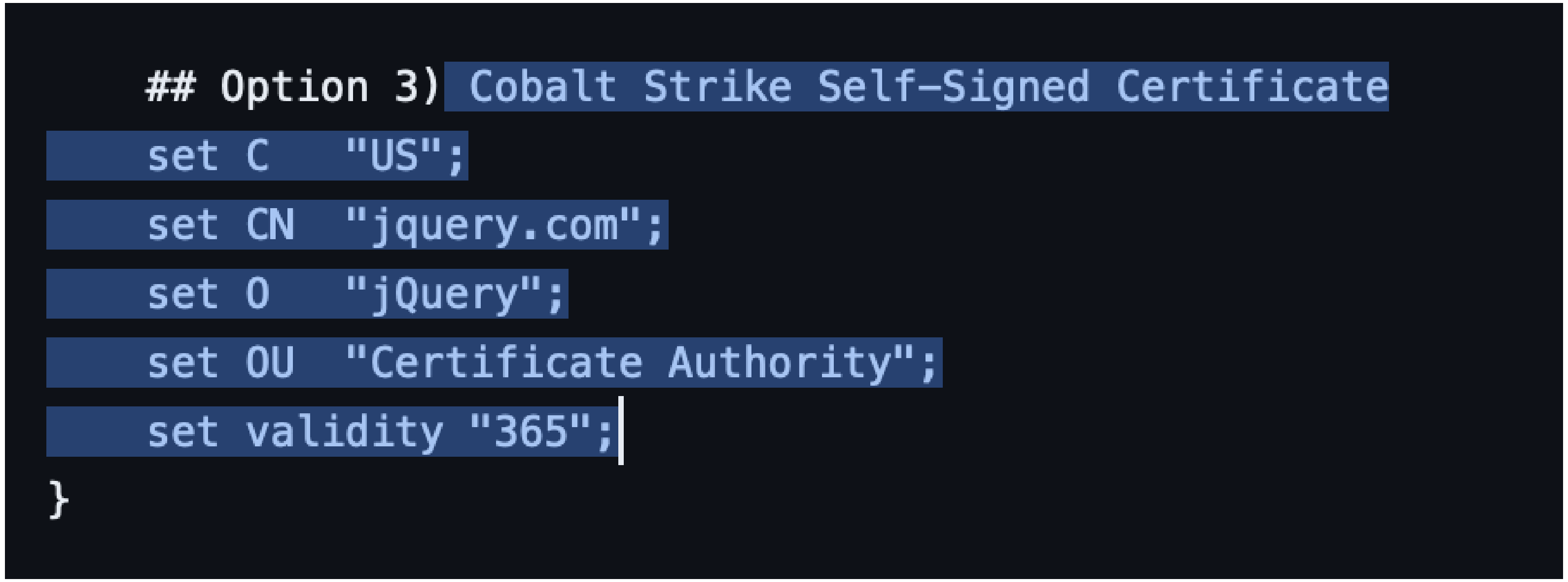
```
# Malleable C2 Profile
# Version: CobaltStrike 4.0
# File: jquery-c2.4.0.profile
# Description:
#    c2 profile attempting to mimic a jquery.js request
#    uses signed certificates
#    or self-signed certificates
```

Cobalt Strike Malleable Profiles

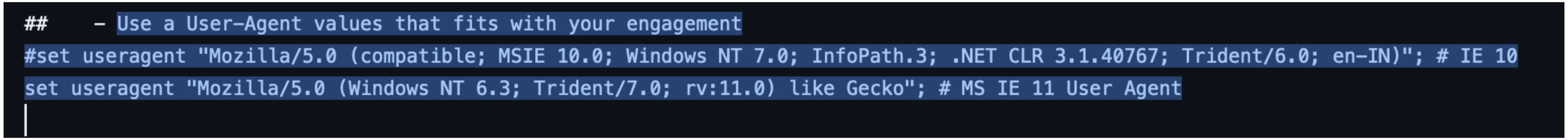


```
header "Server" "NetDNA-cache/2.2";
header "Cache-Control" "max-age=0, no-cache";
header "Pragma" "no-cache";
header "Connection" "keep-alive";
header "Content-Type" "application/javascript; charset=utf-8";
```

Cobalt Strike C2

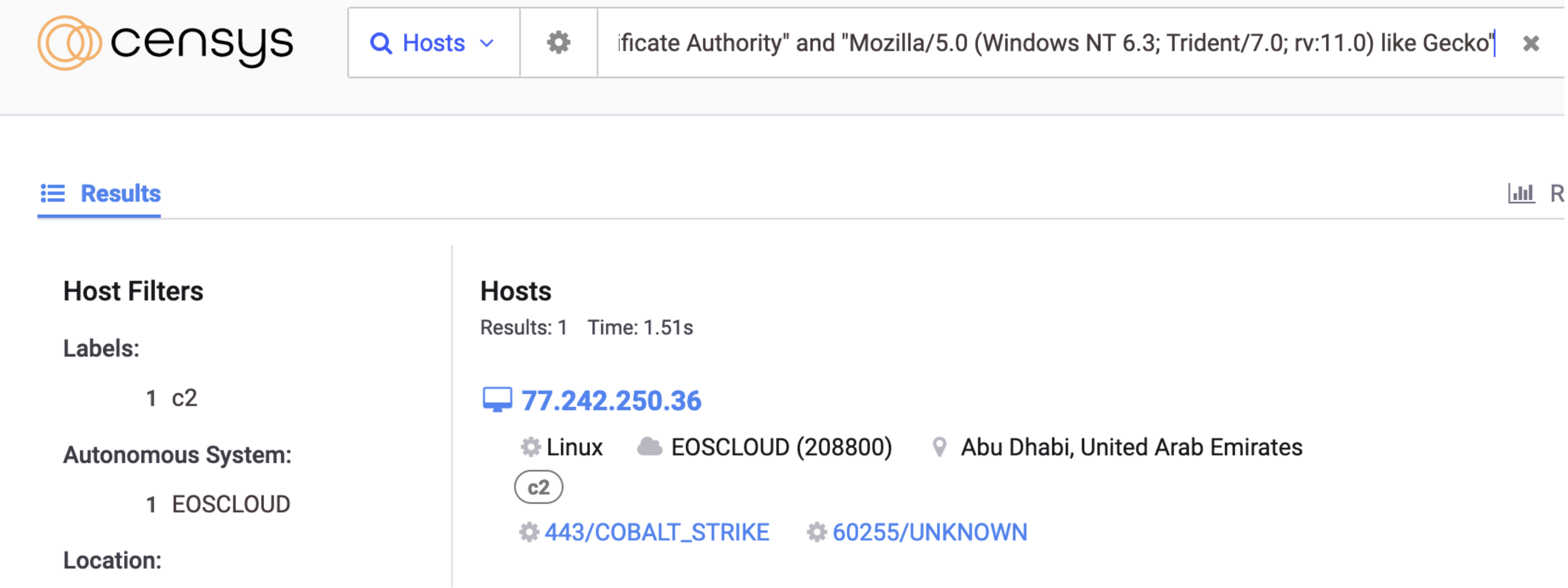


```
    ## Option 3) Cobalt Strike Self-Signed Certificate
    set C   "US";
    set CN  "jquery.com";
    set O   "jQuery";
    set OU  "Certificate Authority";
    set validity "365";
}
```



```
##    - Use a User-Agent values that fits with your engagement
#set useragent "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 7.0; InfoPath.3; .NET CLR 3.1.40767; Trident/6.0; en-IN)"; # IE 10
set useragent "Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko"; # MS IE 11 User Agent
```

Cobalt Strike C2



ificate Authority" and "Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko"

Host Filters

Labels:

1 c2

Autonomous System:

1 EOSCLOUD

Location:

Hosts

Results: 1 Time: 1.51s

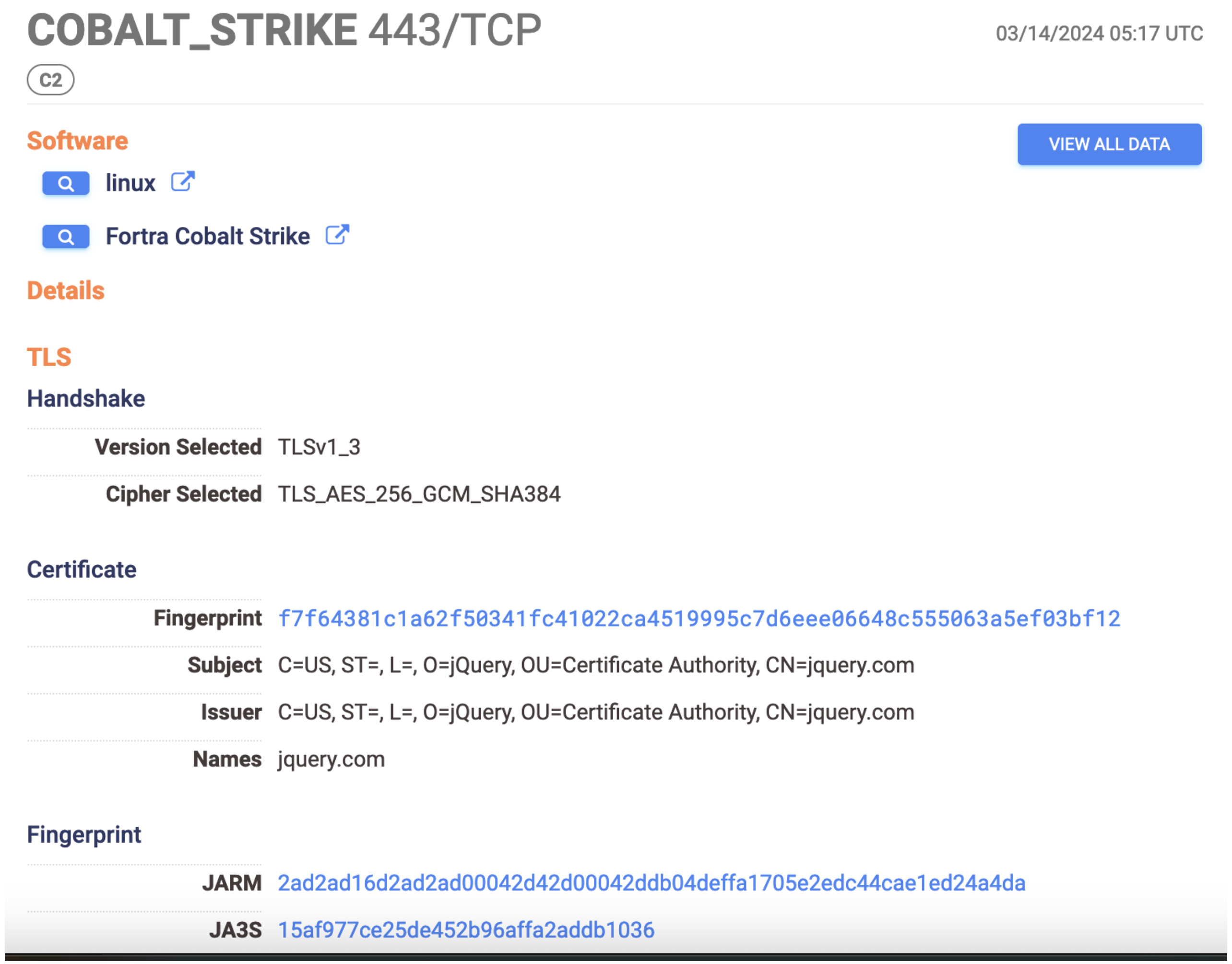
77.242.250.36

Linux EOSCLOUD (208800) Abu Dhabi, United Arab Emirates

c2

443/COBALT_STRIKE 60255/UNKNOWN

Cobalt Strike C2



COBALT_STRIKE 443/TCP

03/14/2024 05:17 UTC

Software

- linux
- Fortra Cobalt Strike

Details

TLS

Handshake

Version Selected	TLSv1_3
Cipher Selected	TLS_AES_256_GCM_SHA384

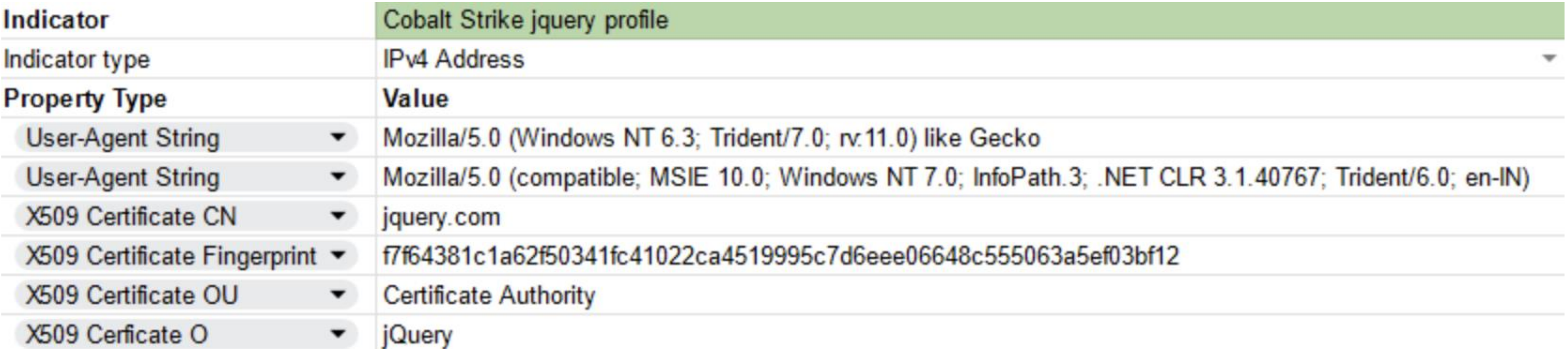
Certificate

Fingerprint	f7f64381c1a62f50341fc41022ca4519995c7d6eee06648c555063a5ef03bf12
Subject	C=US, ST=, L=, O=jQuery, OU=Certificate Authority, CN=jquery.com
Issuer	C=US, ST=, L=, O=jQuery, OU=Certificate Authority, CN=jquery.com
Names	jquery.com

Fingerprint

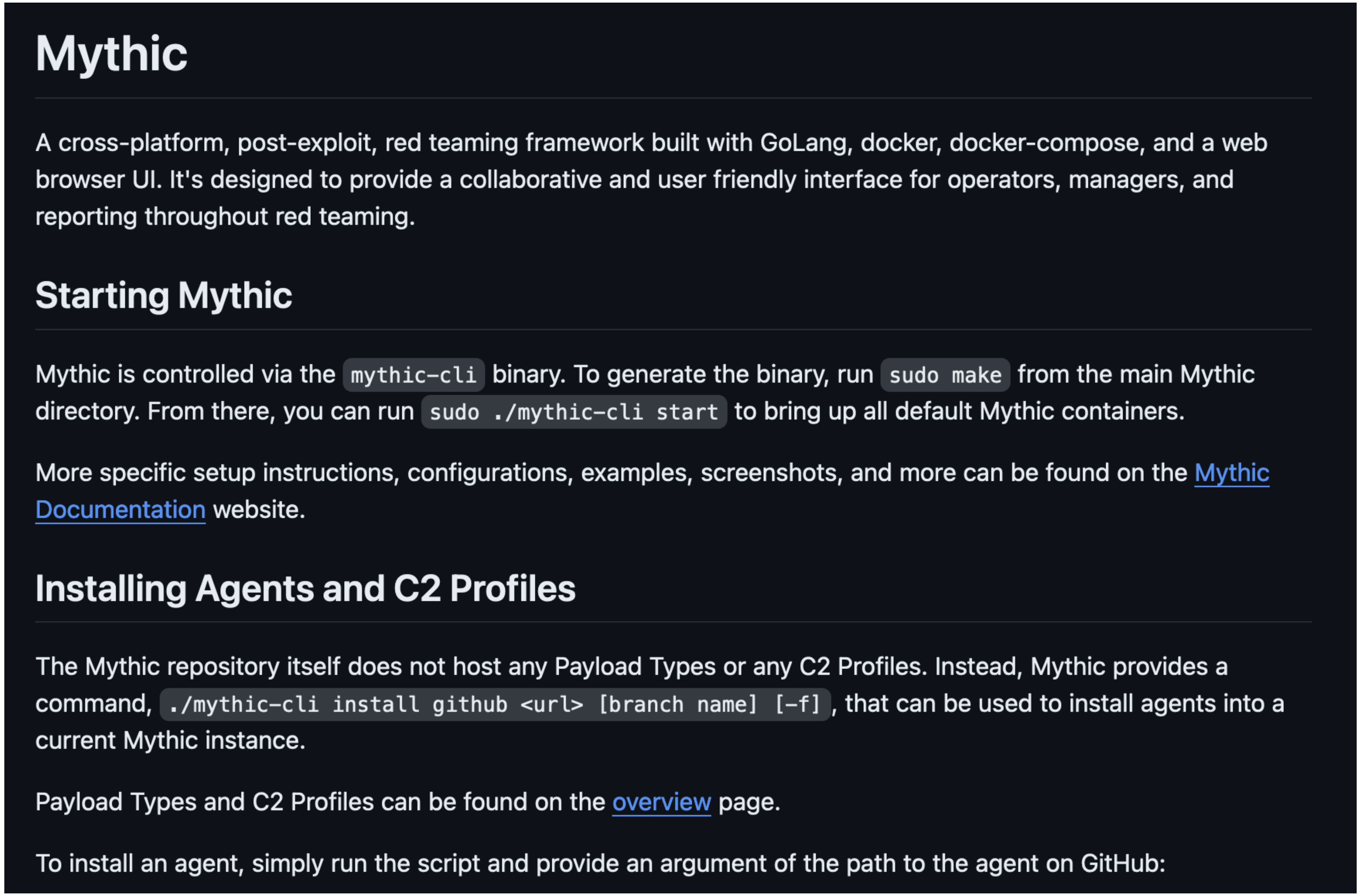
JARM	2ad2ad16d2ad2ad00042d42d00042ddb04deffa1705e2edc44cae1ed24a4da
JA3S	15af977ce25de452b96affa2addb1036

Cobalt Strike C2



Indicator	Cobalt Strike jquery profile
Indicator type	IPv4 Address
Property Type	**Value**
User-Agent String	Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
User-Agent String	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 7.0; InfoPath.3; .NET CLR 3.1.40767; Trident/6.0; en-IN)
X509 Certificate CN	jquery.com
X509 Certificate Fingerprint	f7f64381c1a62f50341fc41022ca4519995c7d6eee06648c555063a5ef03bf12
X509 Certificate OU	Certificate Authority
X509 Cerficate O	jQuery

Mythic C2 Profiling



Mythic

A cross-platform, post-exploit, red teaming framework built with GoLang, docker, docker-compose, and a web browser UI. It's designed to provide a collaborative and user friendly interface for operators, managers, and reporting throughout red teaming.

Starting Mythic

Mythic is controlled via the `mythic-cli` binary. To generate the binary, run `sudo make` from the main Mythic directory. From there, you can run `sudo ./mythic-cli start` to bring up all default Mythic containers.

More specific setup instructions, configurations, examples, screenshots, and more can be found on the Mythic Documentation website.

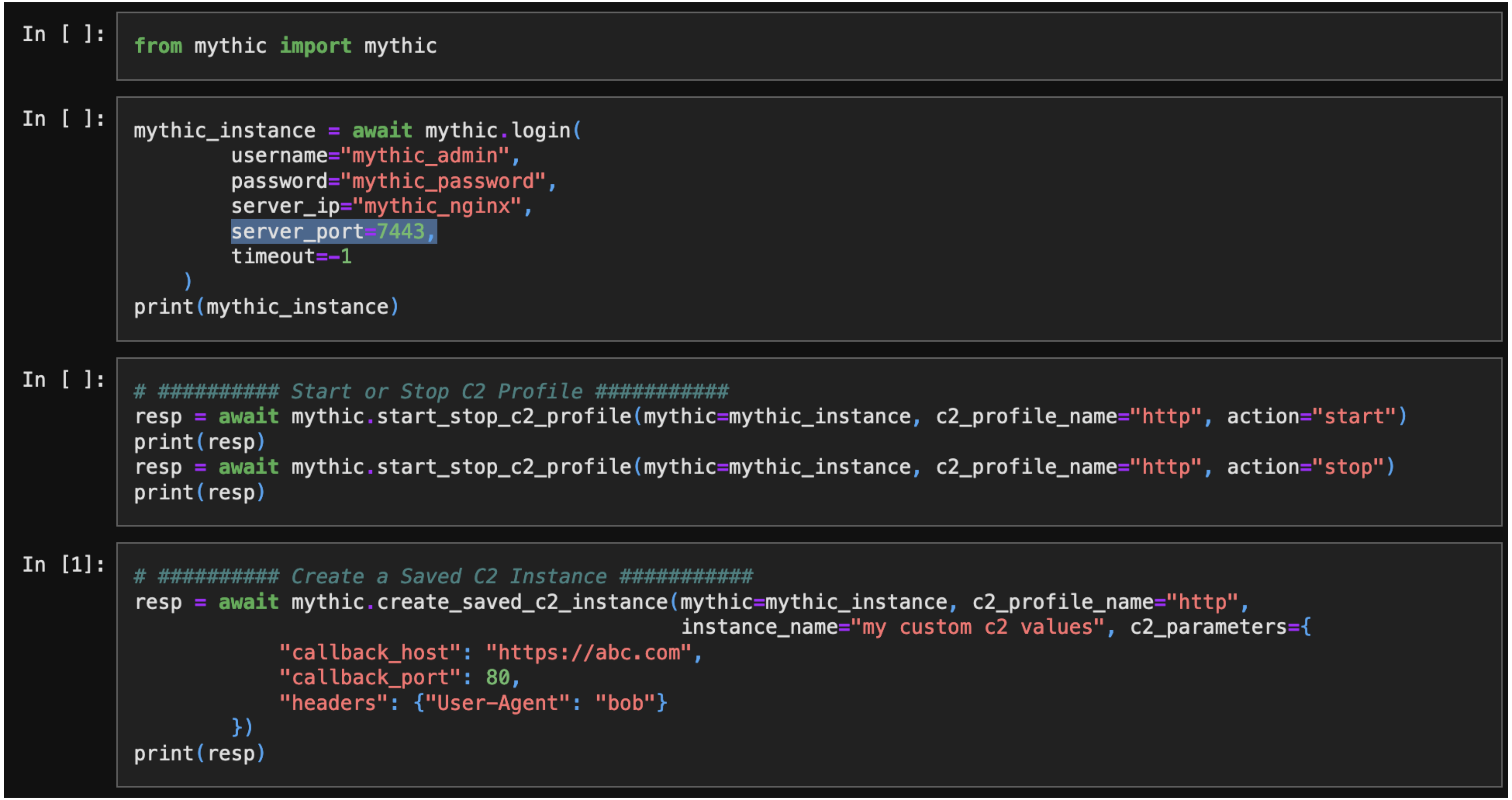
Installing Agents and C2 Profiles

The Mythic repository itself does not host any Payload Types or any C2 Profiles. Instead, Mythic provides a command, `./mythic-cli install github <url> [branch name] [-f]`, that can be used to install agents into a current Mythic instance.

Payload Types and C2 Profiles can be found on the overview page.

To install an agent, simply run the script and provide an argument of the path to the agent on GitHub:

Mythic C2 Profiling



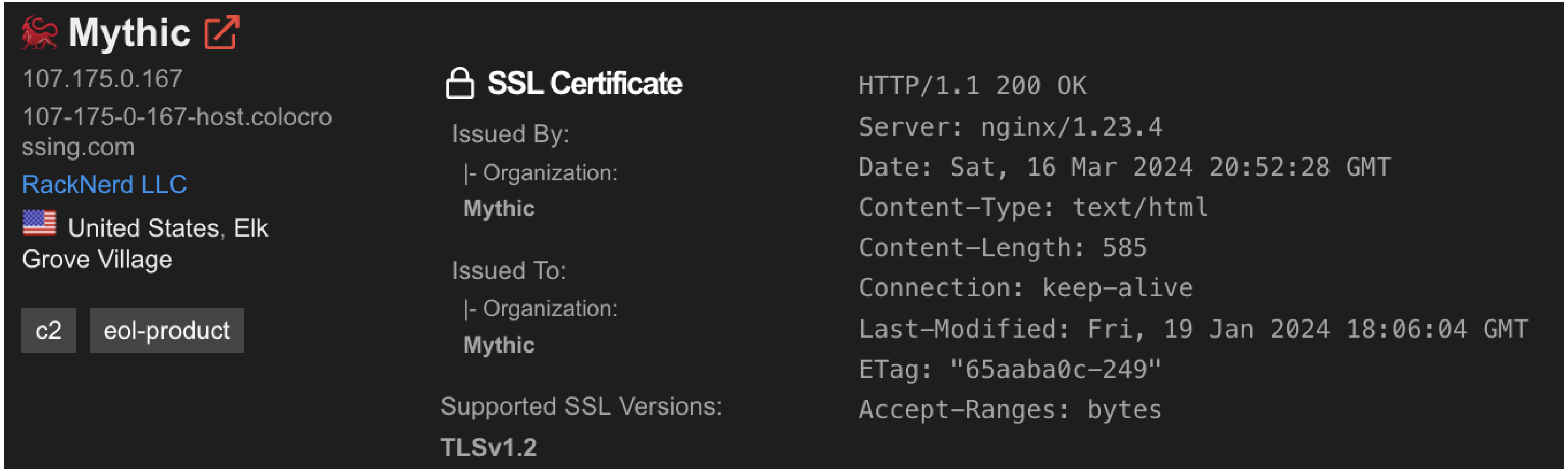
```
In [ ]: from mythic import mythic
```

```
In [ ]: mythic_instance = await mythic.login(
                username="mythic_admin",
                password="mythic_password",
                server_ip="mythic_nginx",
                server_port=7443,
                timeout=-1
            )
        print(mythic_instance)
```

```
In [ ]: # ########## Start or Stop C2 Profile ###########
        resp = await mythic.start_stop_c2_profile(mythic=mythic_instance, c2_profile_name="http", action="start")
        print(resp)
        resp = await mythic.start_stop_c2_profile(mythic=mythic_instance, c2_profile_name="http", action="stop")
        print(resp)
```

```
In [1]: # ########## Create a Saved C2 Instance ###########
        resp = await mythic.create_saved_c2_instance(mythic=mythic_instance, c2_profile_name="http",
                                                     instance_name="my custom c2 values", c2_parameters={
                    "callback_host": "https://abc.com",
                    "callback_port": 80,
                    "headers": {"User-Agent": "bob"}
                })
        print(resp)
```

Mythic C2 Profiling



Mythic

107.175.0.167

107-175-0-167-host.colocrossing.com

RackNerd LLC

United States, Elk Grove Village

c2 eol-product

SSL Certificate

Issued By:

|- Organization:

Mythic

Issued To:

|- Organization:

Mythic

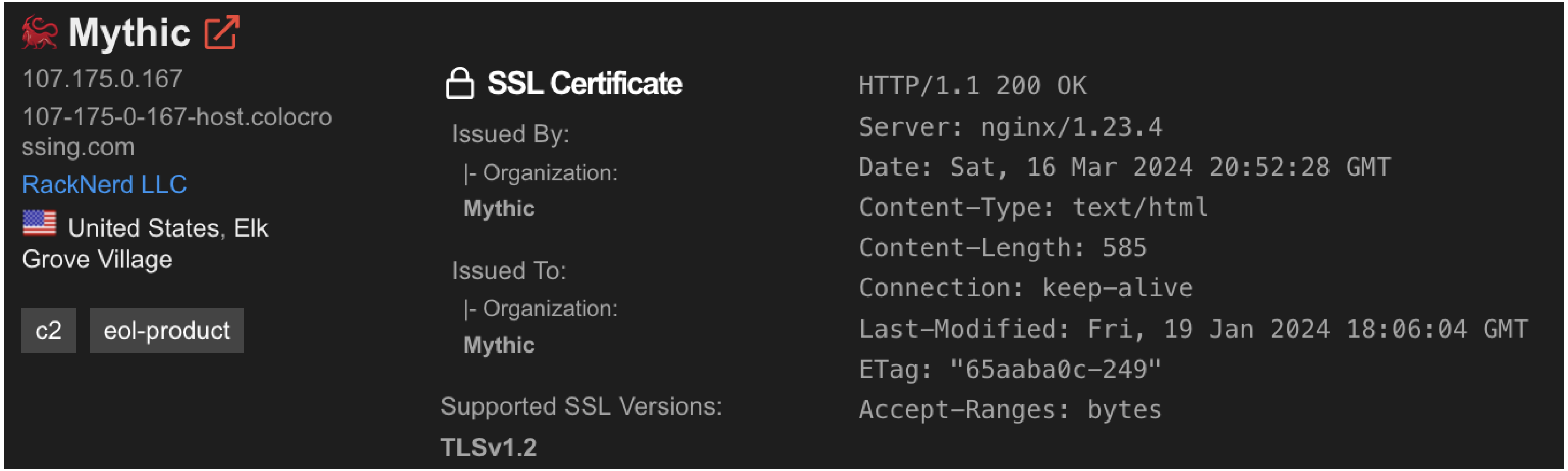
Supported SSL Versions:

TLSv1.2

```
HTTP/1.1 200 OK
Server: nginx/1.23.4
Date: Sat, 16 Mar 2024 20:52:28 GMT
Content-Type: text/html
Content-Length: 585
Connection: keep-alive
Last-Modified: Fri, 19 Jan 2024 18:06:04 GMT
ETag: "65aaba0c-249"
Accept-Ranges: bytes
```

PUBLIC

Mythic C2 Profiling



Mythic

107.175.0.167

107-175-0-167-host.colocrossing.com

RackNerd LLC

🇺🇸 United States, Elk Grove Village

c2 eol-product

SSL Certificate

Issued By:

|- Organization:

Mythic

Issued To:

|- Organization:

Mythic

Supported SSL Versions:

TLSv1.2

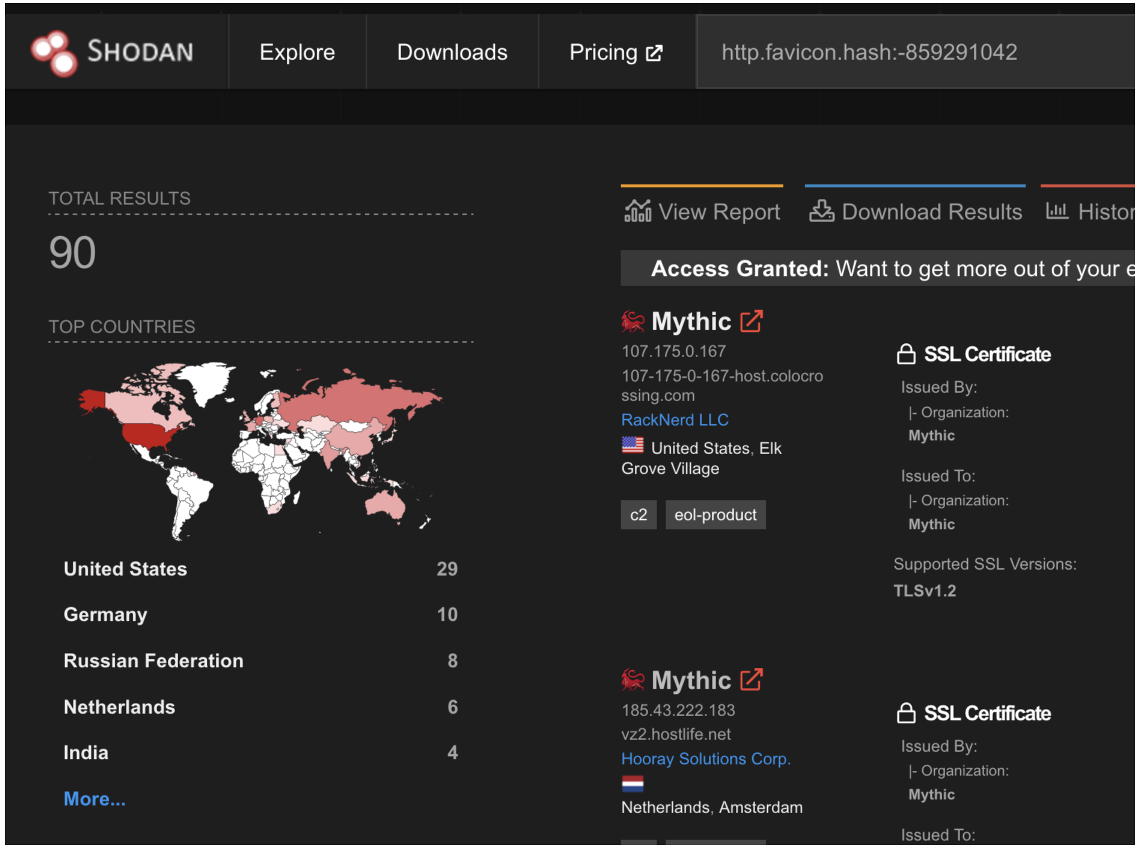
```
HTTP/1.1 200 OK
Server: nginx/1.23.4
Date: Sat, 16 Mar 2024 20:52:28 GMT
Content-Type: text/html
Content-Length: 585
Connection: keep-alive
Last-Modified: Fri, 19 Jan 2024 18:06:04 GMT
ETag: "65aaba0c-249"
Accept-Ranges: bytes
```

Favicon

Certificate

Headers (values + headers hash)

Mythic C2 Profiling



http.favicon.hash:-859291042

TOTAL RESULTS

90

TOP COUNTRIES

United States	29
Germany	10
Russian Federation	8
Netherlands	6
India	4

More...

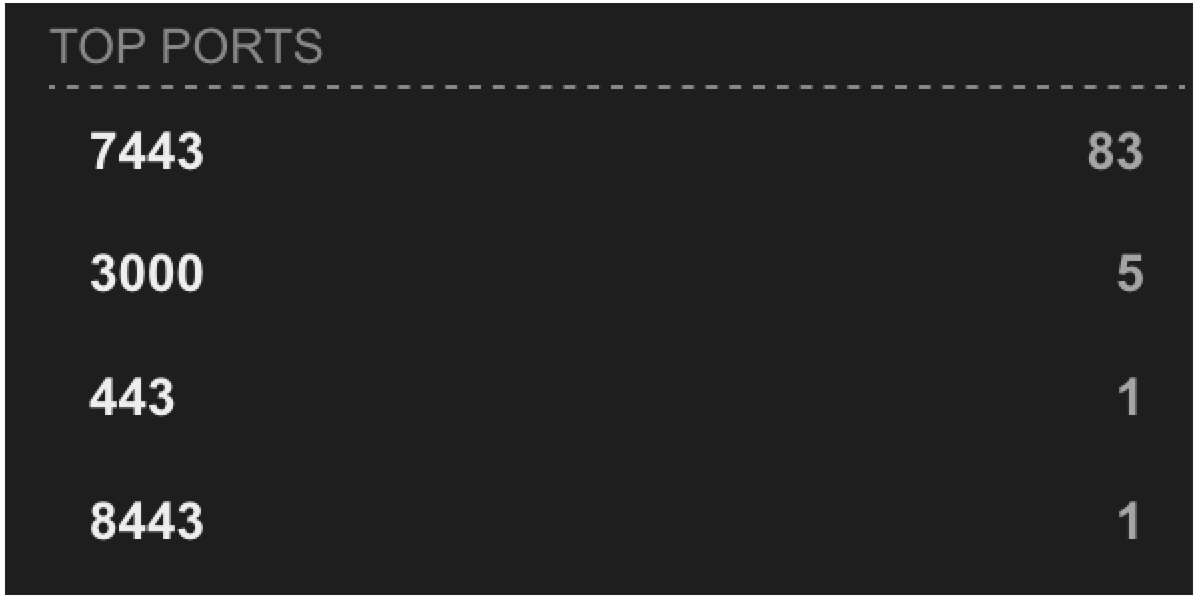
Access Granted: Want to get more out of your e

Mythic
107.175.0.167
107-175-0-167-host.colocrossing.com
RackNerd LLC
United States, Elk Grove Village
c2 eol-product

SSL Certificate
Issued By:
|- Organization:
Mythic
Issued To:
|- Organization:
Mythic
Supported SSL Versions:
TLSv1.2

Mythic
185.43.222.183
vz2.hostlife.net
Hooray Solutions Corp.
Netherlands, Amsterdam

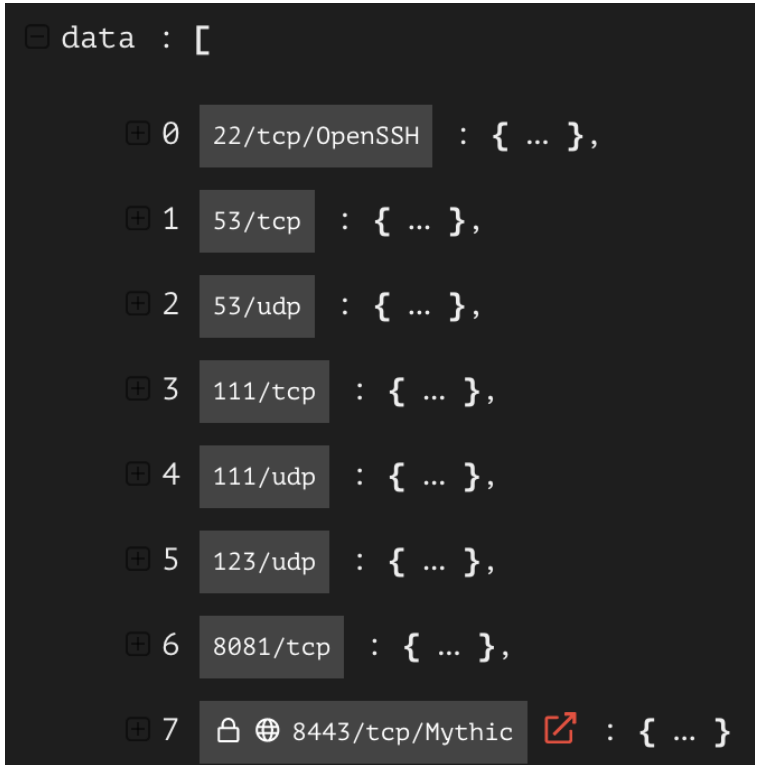
SSL Certificate
Issued By:
|- Organization:
Mythic
Issued To:



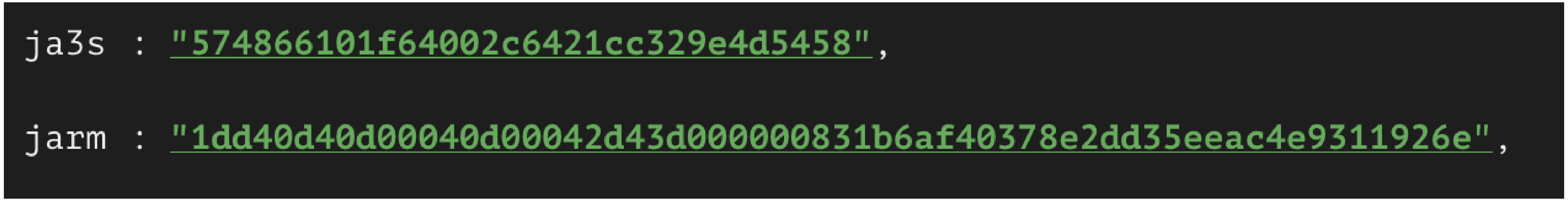
TOP PORTS

7443	83
3000	5
443	1
8443	1

Mythic C2 Profiling

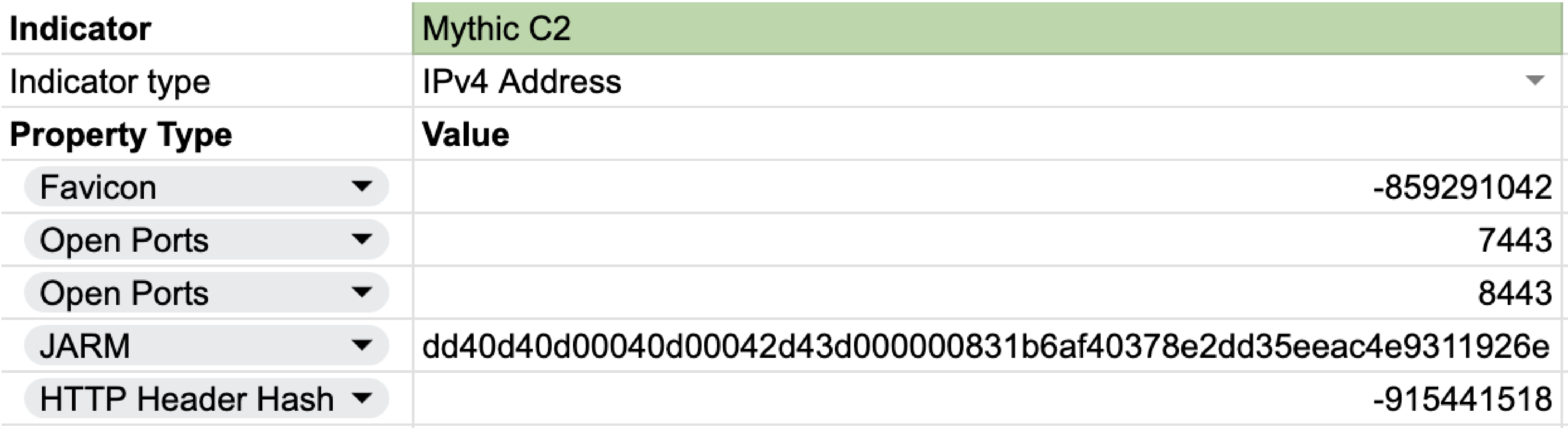


```
data : [
    0  22/tcp/OpenSSH  : { … },
    1  53/tcp  : { … },
    2  53/udp  : { … },
    3  111/tcp  : { … },
    4  111/udp  : { … },
    5  123/udp  : { … },
    6  8081/tcp  : { … },
    7  8443/tcp/Mythic  : { … }
```



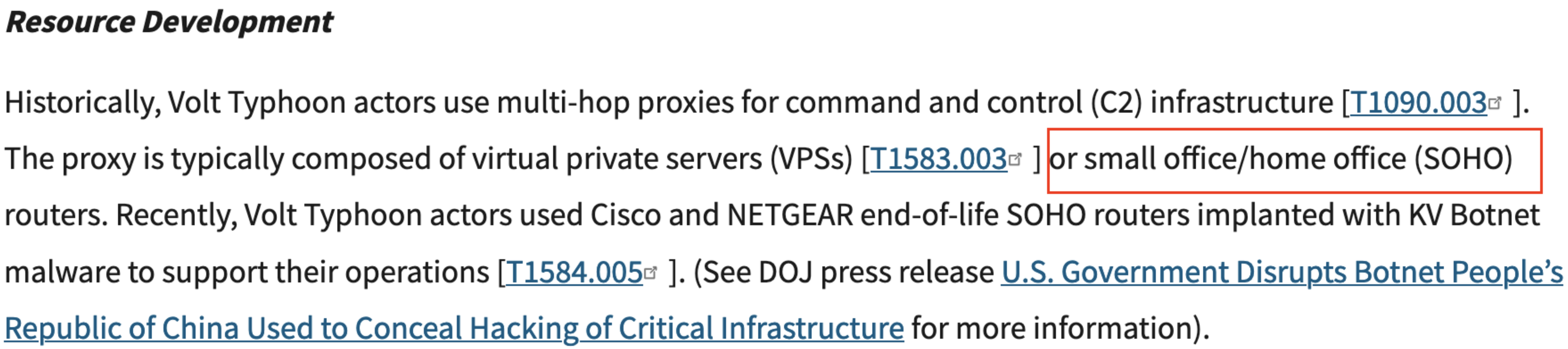
```
ja3s : "574866101f64002c6421cc329e4d5458",

jarm : "1dd40d40d00040d00042d43d000000831b6af40378e2dd35eeac4e9311926e",
```

Mythic C2 Profiling



Indicator	Mythic C2
Indicator type	IPv4 Address
Property Type	**Value**
Favicon	-859291042
Open Ports	7443
Open Ports	8443
JARM	dd40d40d00040d00042d43d000000831b6af40378e2dd35eeac4e9311926e
HTTP Header Hash	-915441518

Volt Typhoon

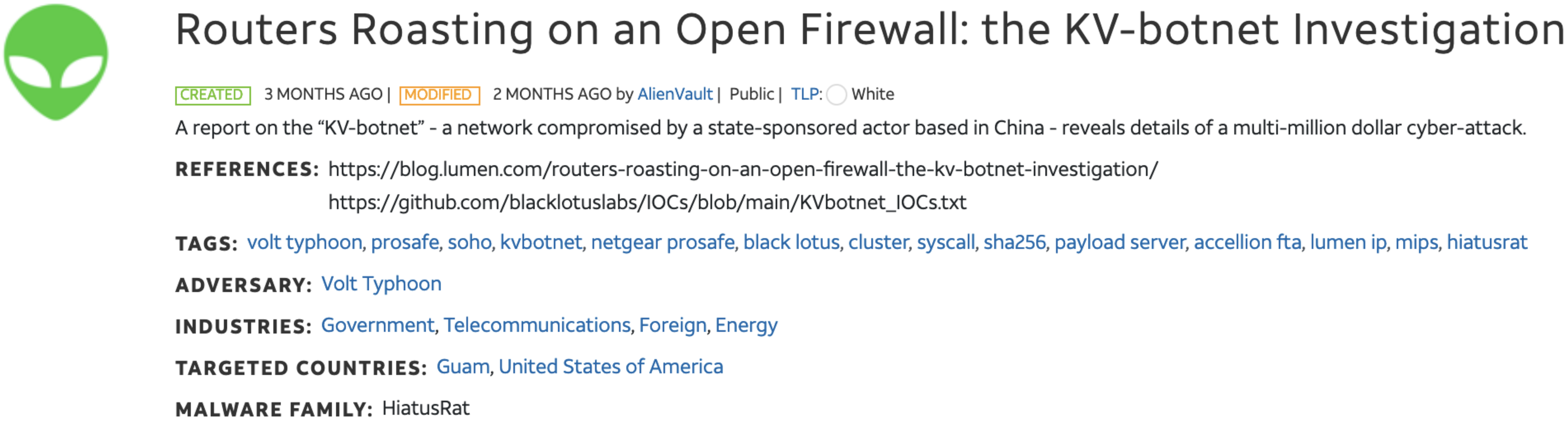


Resource Development

Historically, Volt Typhoon actors use multi-hop proxies for command and control (C2) infrastructure [T1090.003]. The proxy is typically composed of virtual private servers (VPSs) [T1583.003] or small office/home office (SOHO) routers. Recently, Volt Typhoon actors used Cisco and NETGEAR end-of-life SOHO routers implanted with KV Botnet malware to support their operations [T1584.005]. (See DOJ press release U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure for more information).

Picture source: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

Volt Typhoon



Routers Roasting on an Open Firewall: the KV-botnet Investigation

CREATED 3 MONTHS AGO | MODIFIED 2 MONTHS AGO by AlienVault | Public | TLP: ○ White

A report on the “KV-botnet” - a network compromised by a state-sponsored actor based in China - reveals details of a multi-million dollar cyber-attack.

REFERENCES: https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/
https://github.com/blacklotuslabs/IOCs/blob/main/KVbotnet_IOCs.txt

TAGS: volt typhoon, prosafe, soho, kvbotnet, netgear prosafe, black lotus, cluster, syscall, sha256, payload server, accellion fta, lumen ip, mips, hiatusrat

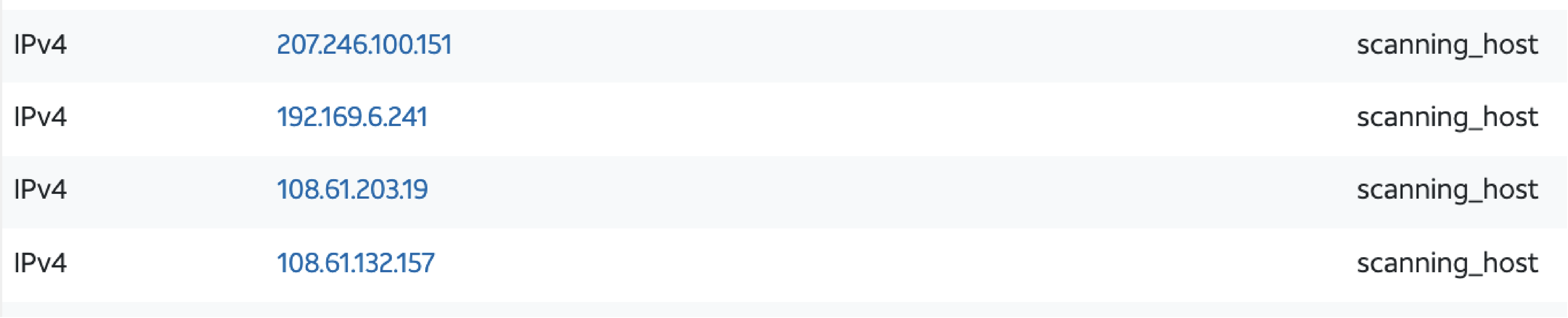
ADVERSARY: Volt Typhoon

INDUSTRIES: Government, Telecommunications, Foreign, Energy

TARGETED COUNTRIES: Guam, United States of America

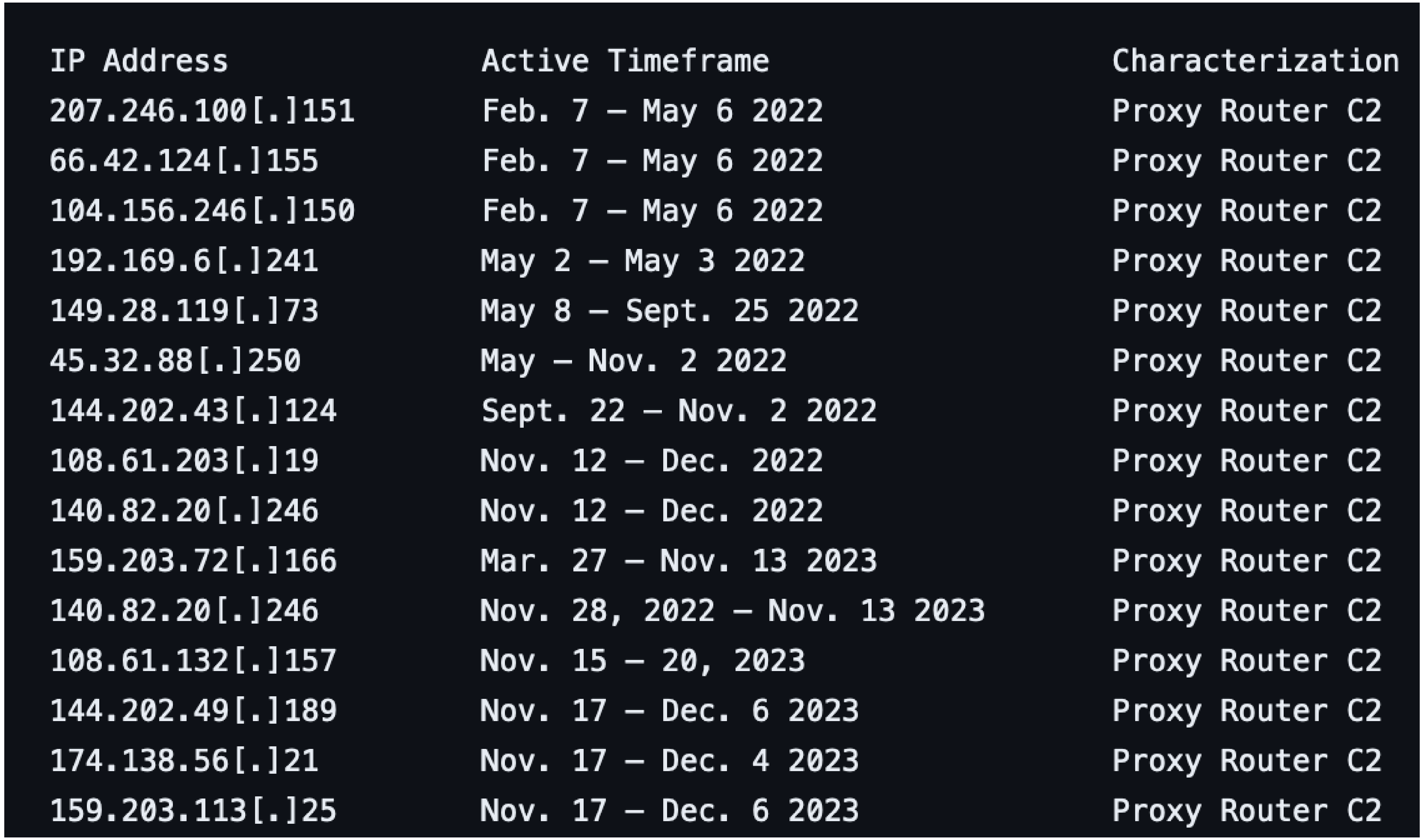
MALWARE FAMILY: HiatusRat

Volt Typhoon



IPv4	207.246.100.151	scanning_host
IPv4	192.169.6.241	scanning_host
IPv4	108.61.203.19	scanning_host
IPv4	108.61.132.157	scanning_host

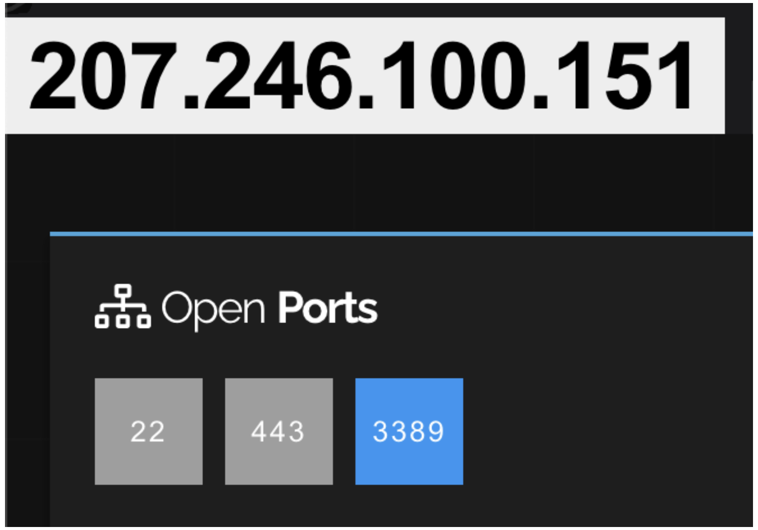
Volt Typhoon



IP Address	Active Timeframe	Characterization
207.246.100[.]151	Feb. 7 – May 6 2022	Proxy Router C2
66.42.124[.]155	Feb. 7 – May 6 2022	Proxy Router C2
104.156.246[.]150	Feb. 7 – May 6 2022	Proxy Router C2
192.169.6[.]241	May 2 – May 3 2022	Proxy Router C2
149.28.119[.]73	May 8 – Sept. 25 2022	Proxy Router C2
45.32.88[.]250	May – Nov. 2 2022	Proxy Router C2
144.202.43[.]124	Sept. 22 – Nov. 2 2022	Proxy Router C2
108.61.203[.]19	Nov. 12 – Dec. 2022	Proxy Router C2
140.82.20[.]246	Nov. 12 – Dec. 2022	Proxy Router C2
159.203.72[.]166	Mar. 27 – Nov. 13 2023	Proxy Router C2
140.82.20[.]246	Nov. 28, 2022 – Nov. 13 2023	Proxy Router C2
108.61.132[.]157	Nov. 15 – 20, 2023	Proxy Router C2
144.202.49[.]189	Nov. 17 – Dec. 6 2023	Proxy Router C2
174.138.56[.]21	Nov. 17 – Dec. 4 2023	Proxy Router C2
159.203.113[.]25	Nov. 17 – Dec. 6 2023	Proxy Router C2

Picture source: https://github.com/blacklotuslabs/IOCs/blob/main/KVbotnet_IOCs.txt

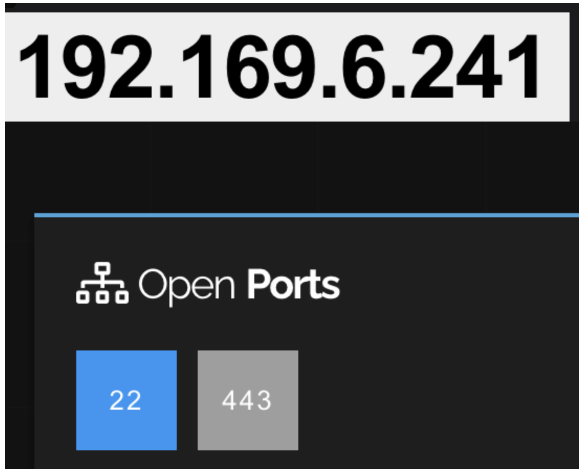
Volt Typhoon



207.246.100.151

Open Ports

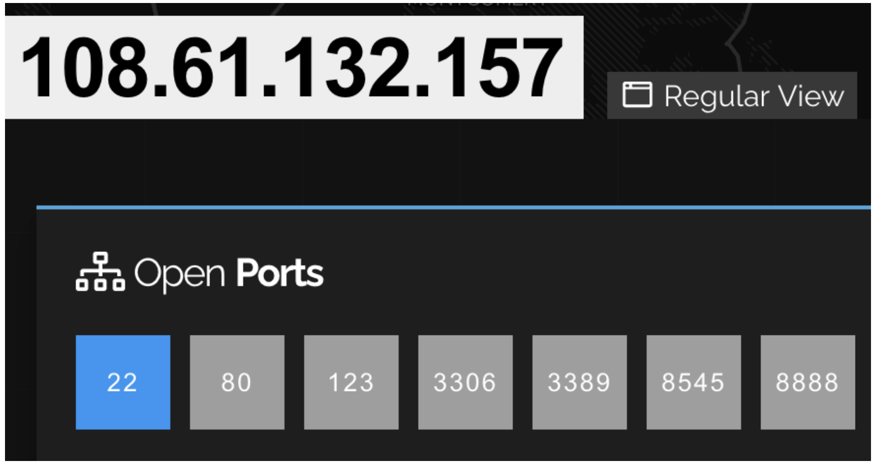
22 443 3389



192.169.6.241

Open Ports

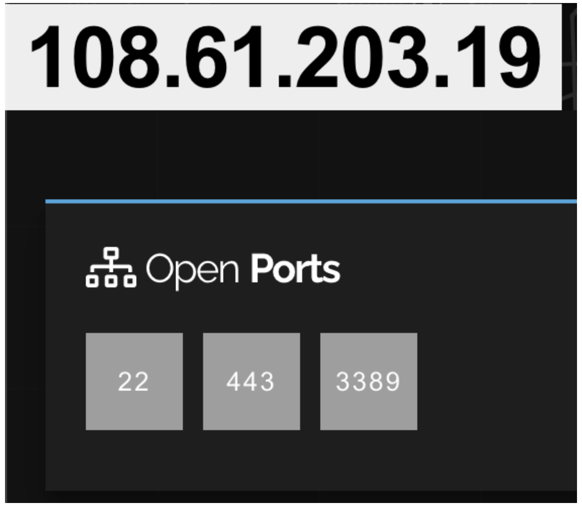
22 443



108.61.132.157

Open Ports

22 80 123 3306 3389 8545 8888

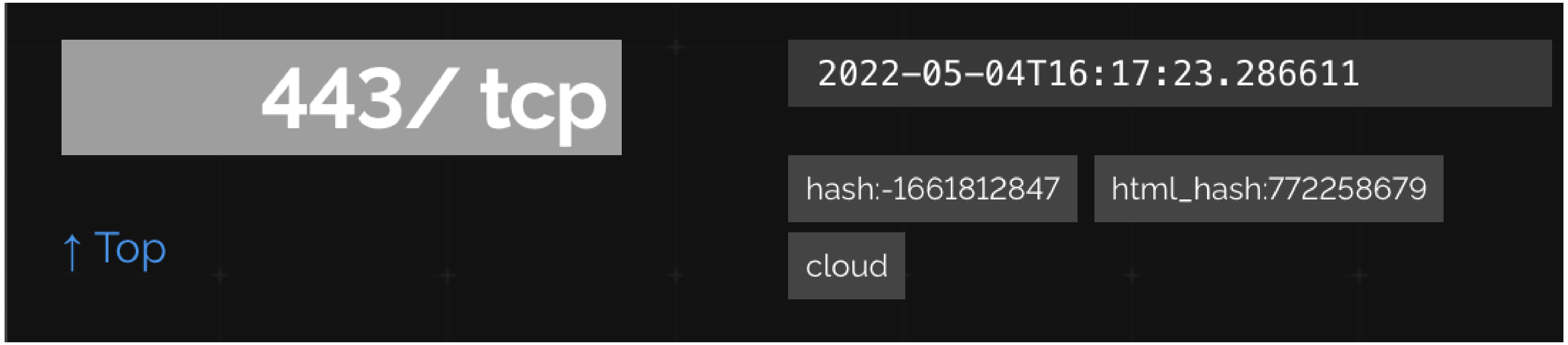


108.61.203.19

Open Ports

22 443 3389

Volt Typhoon



443/ tcp

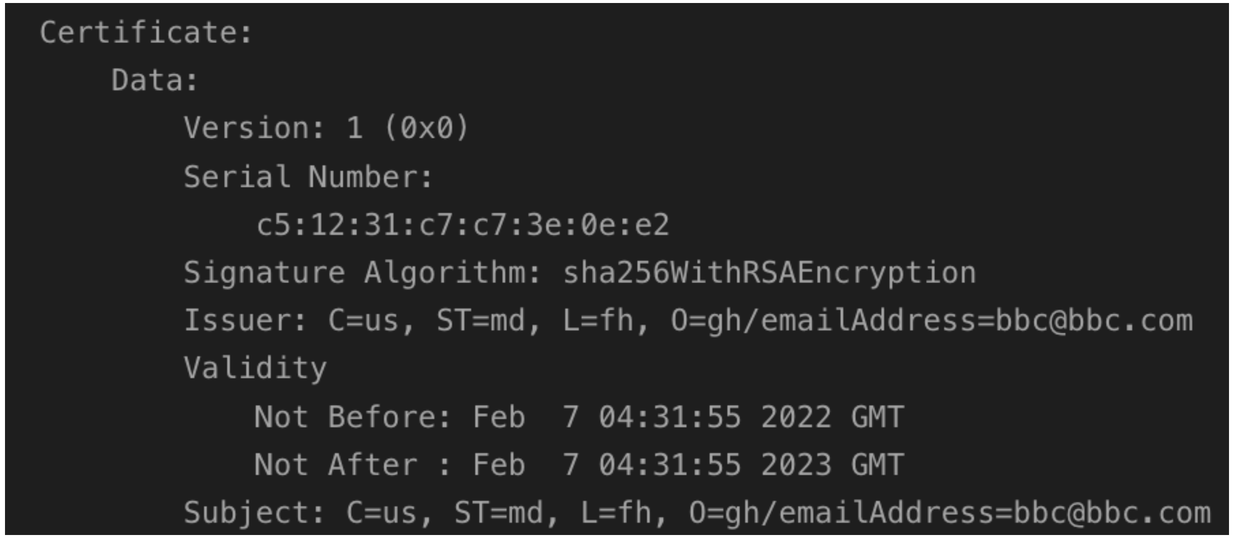
↑ Top

2022-05-04T16:17:23.286611

hash:-1661812847

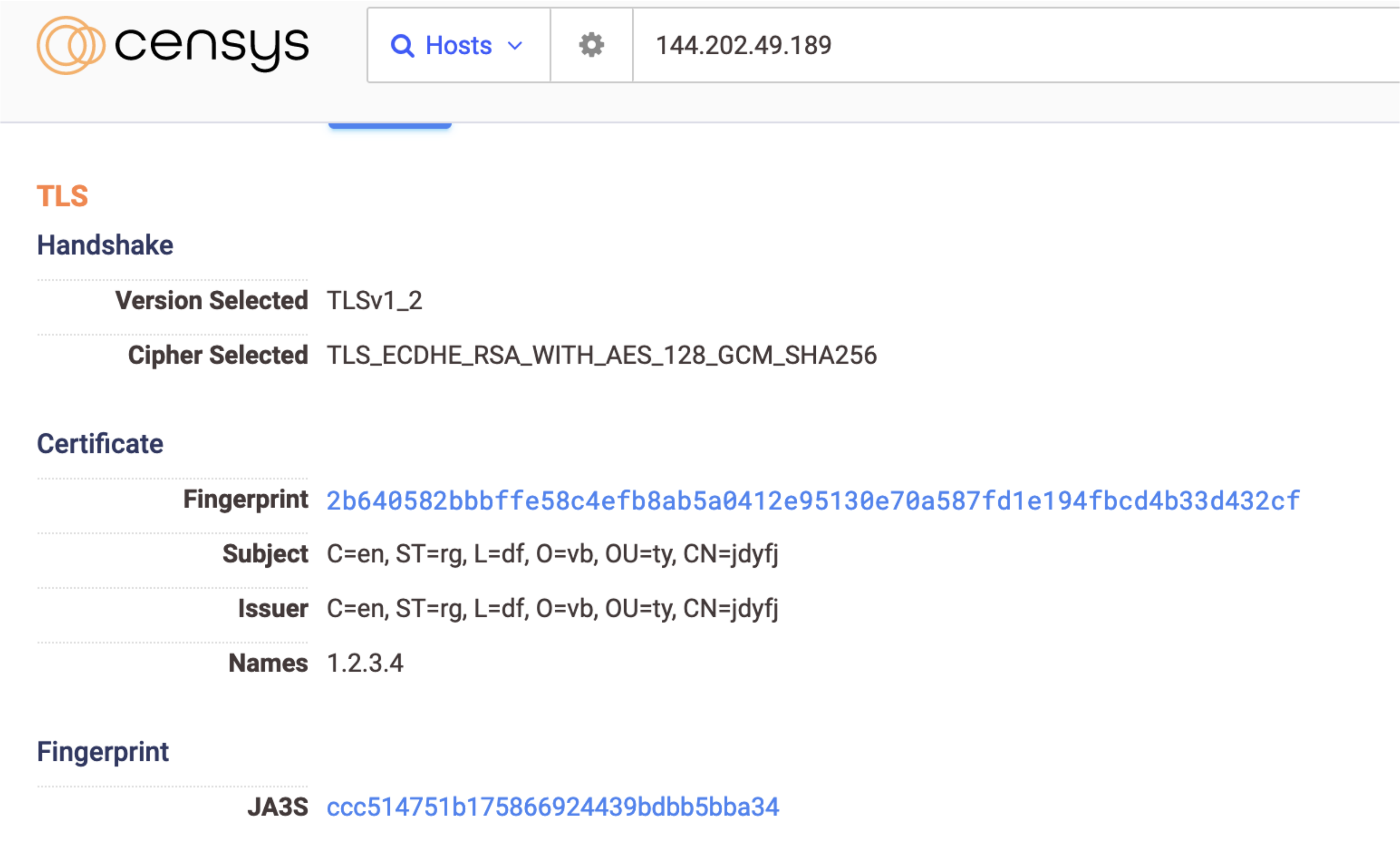
html_hash:772258679

cloud



```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            c5:12:31:c7:c7:3e:0e:e2
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=us, ST=md, L=fh, O=gh/emailAddress=bbc@bbc.com
        Validity
            Not Before: Feb  7 04:31:55 2022 GMT
            Not After : Feb  7 04:31:55 2023 GMT
        Subject: C=us, ST=md, L=fh, O=gh/emailAddress=bbc@bbc.com
```

Volt Typhoon



144.202.49.189

TLS

Handshake

Version Selected TLSv1_2

Cipher Selected TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Certificate

Fingerprint 2b640582bbbffe58c4efb8ab5a0412e95130e70a587fd1e194fbcd4b33d432cf

Subject C=en, ST=rg, L=df, O=vb, OU=ty, CN=jdyfj

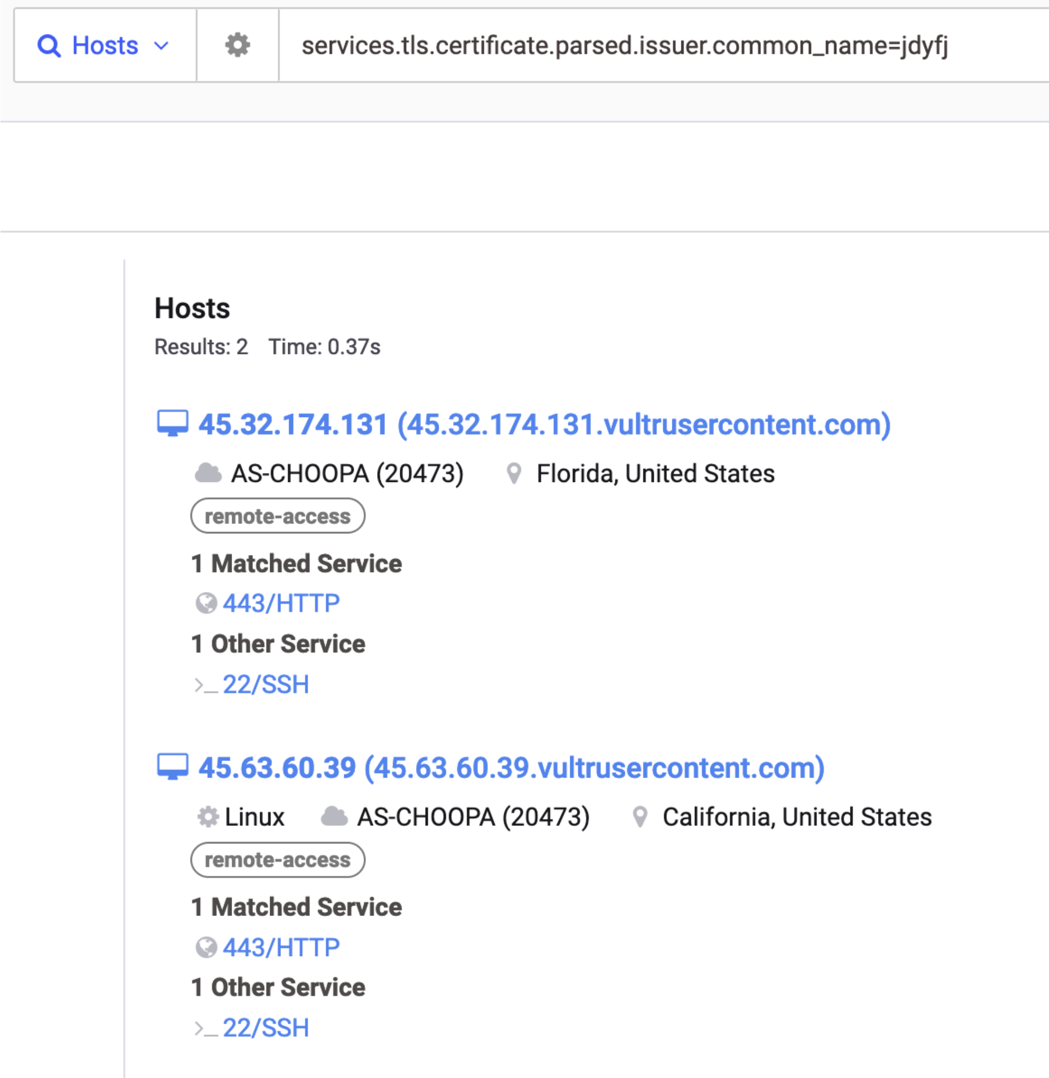
Issuer C=en, ST=rg, L=df, O=vb, OU=ty, CN=jdyfj

Names 1.2.3.4

Fingerprint

JA3S ccc514751b175866924439bdbb5bba34

Volt Typhoon



services.tls.certificate.parsed.issuer.common_name=jdyfj

Hosts

Results: 2 Time: 0.37s

45.32.174.131 (45.32.174.131.vultrusercontent.com)

AS-CHOOPA (20473) Florida, United States

remote-access

1 Matched Service

443/HTTP

1 Other Service

22/SSH

45.63.60.39 (45.63.60.39.vultrusercontent.com)

Linux AS-CHOOPA (20473) California, United States

remote-access

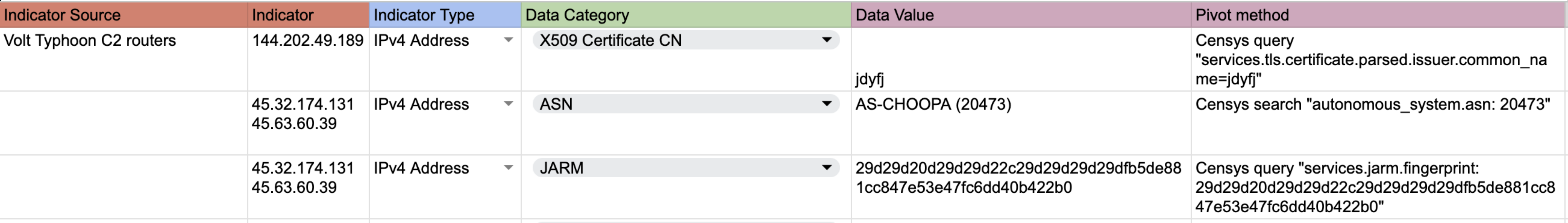
1 Matched Service

443/HTTP

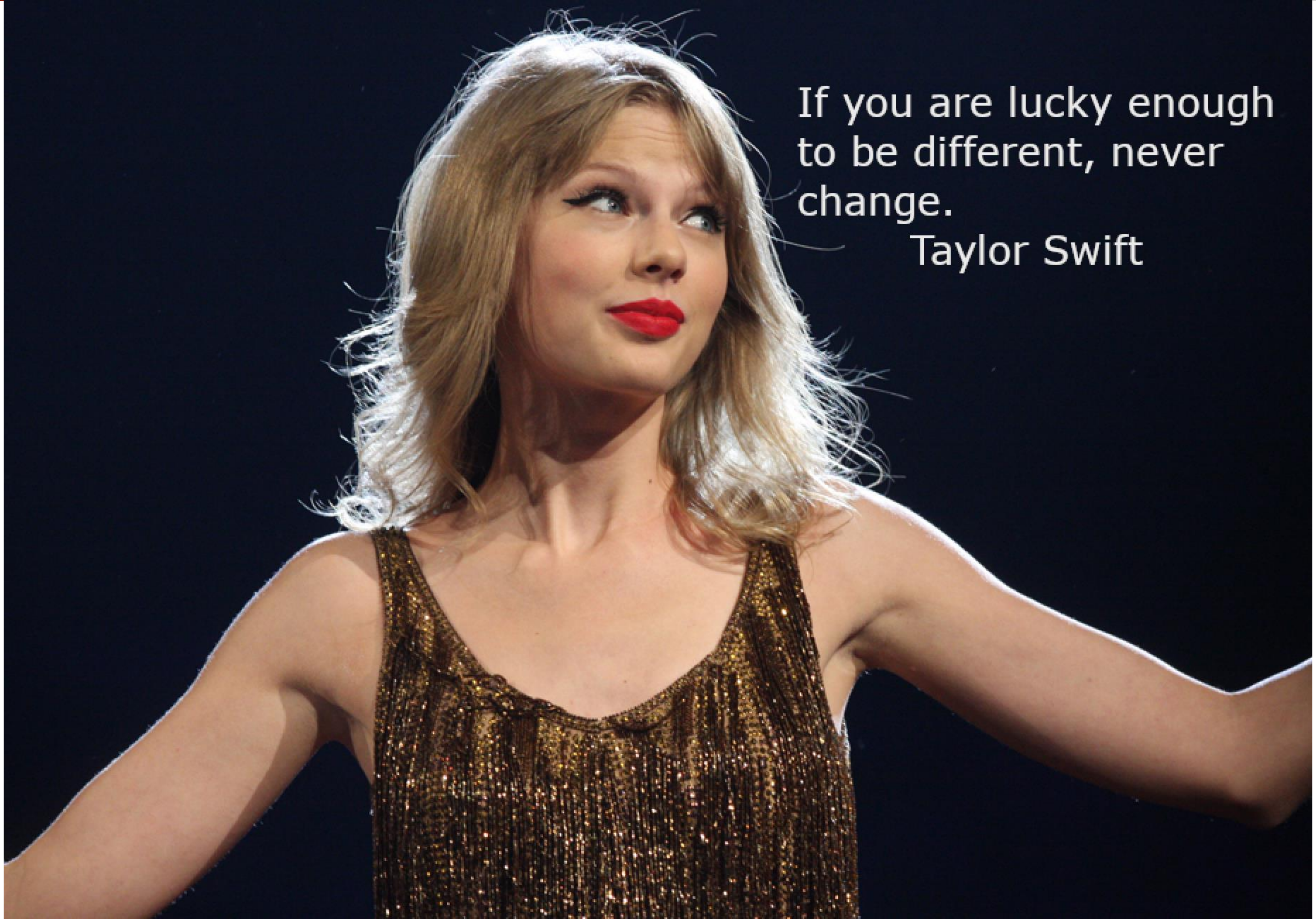
1 Other Service

22/SSH

Volt Typhoon



Indicator Source	Indicator	Indicator Type	Data Category	Data Value	Pivot method
Volt Typhoon C2 routers	144.202.49.189	IPv4 Address	X509 Certificate CN	jdyfj	Censys query "services.tls.certificate.parsed.issuer.common_name=jdyfj"
	45.32.174.131 45.63.60.39	IPv4 Address	ASN	AS-CHOOPA (20473)	Censys search "autonomous_system.asn: 20473"
	45.32.174.131 45.63.60.39	IPv4 Address	JARM	29d29d20d29d29d22c29d29d29d29dfb5de881cc847e53e47fc6dd40b422b0	Censys query "services.jarm.fingerprint: 29d29d20d29d29d22c29d29d29d29dfb5de881cc847e53e47fc6dd40b422b0"

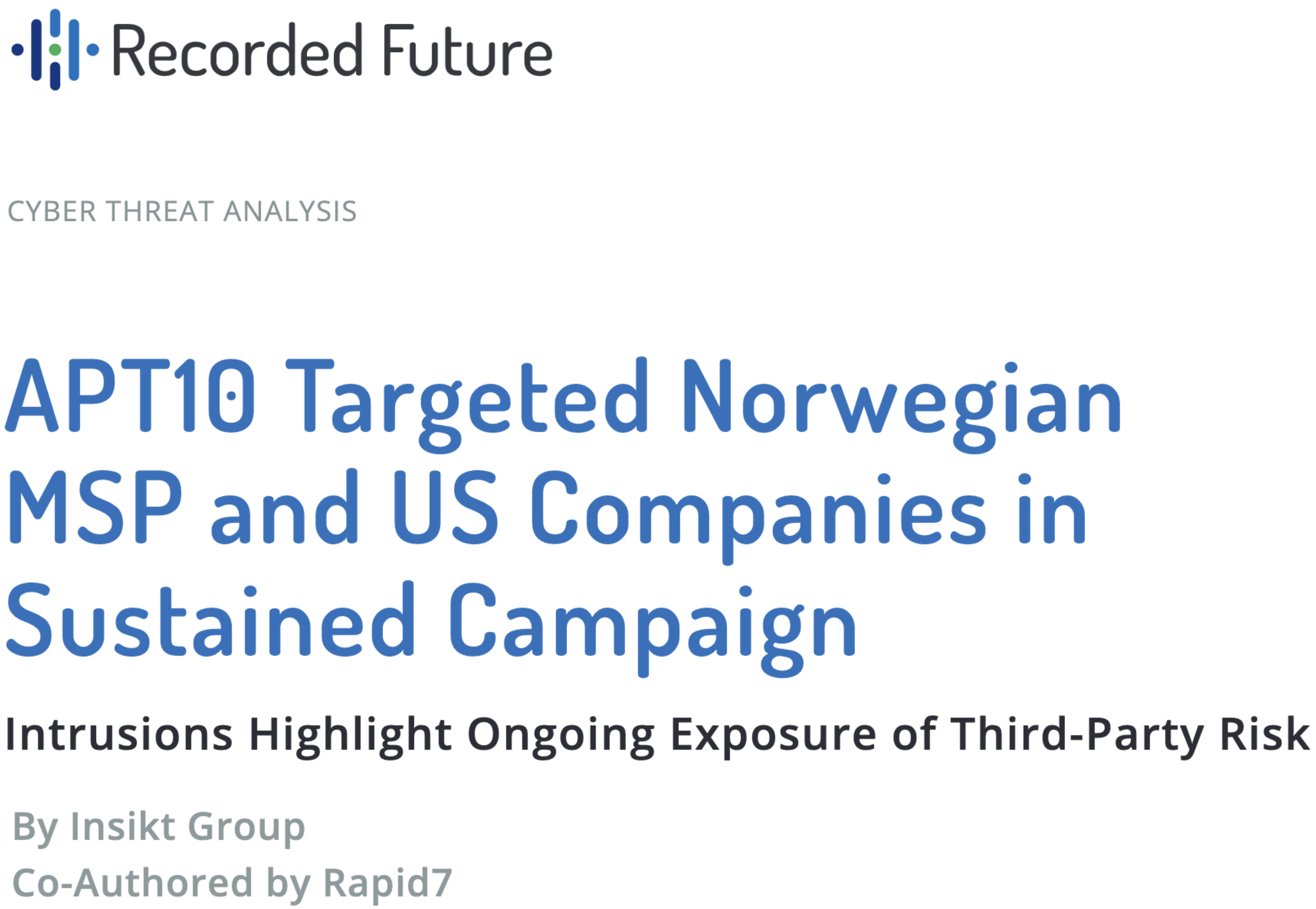


If you are lucky enough to be different, never change.

Taylor Swift

Photograph source: https://www.flickr.com/photos/evarinaldiphotography/6966830273

Infrastructure Tracking and Attribution



Recorded Future

CYBER THREAT ANALYSIS

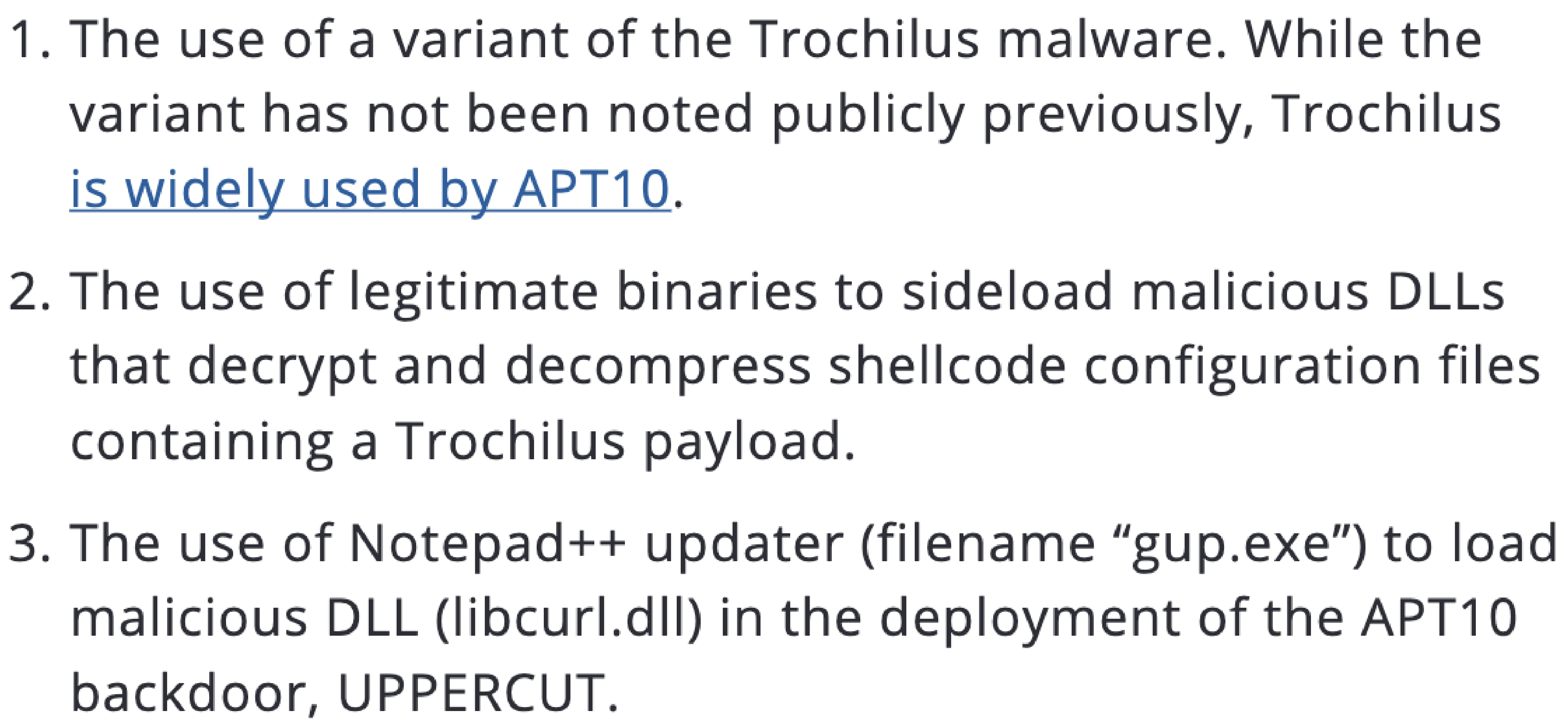
APT10 Targeted Norwegian MSP and US Companies in Sustained Campaign

Intrusions Highlight Ongoing Exposure of Third-Party Risk

By Insikt Group
Co-Authored by Rapid7

Picture source: https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf

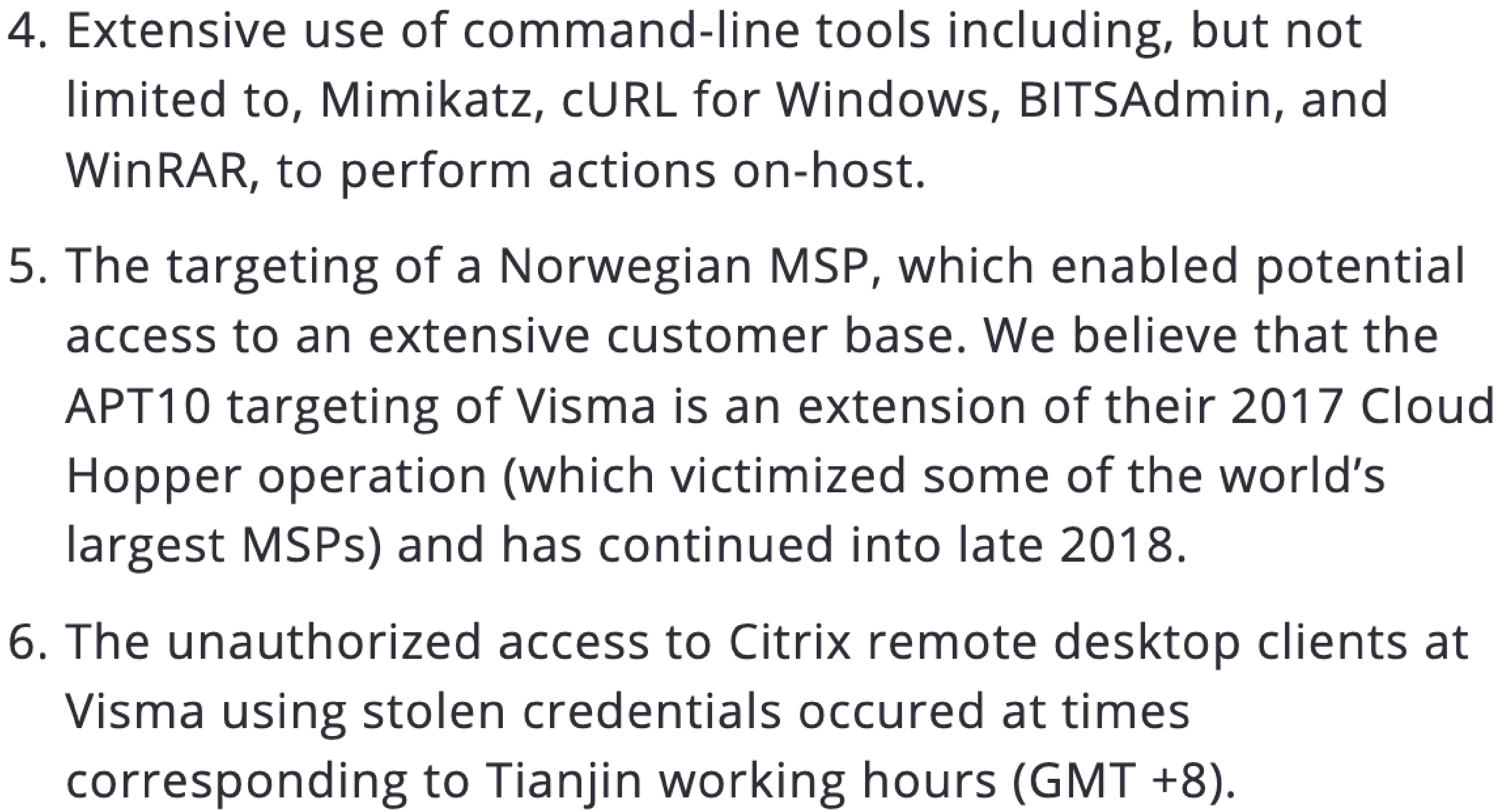
Infrastructure Tracking and Attribution



1. The use of a variant of the Trochilus malware. While the variant has not been noted publicly previously, Trochilus is widely used by APT10.
2. The use of legitimate binaries to sideload malicious DLLs that decrypt and decompress shellcode configuration files containing a Trochilus payload.
3. The use of Notepad++ updater (filename “gup.exe”) to load malicious DLL (libcurl.dll) in the deployment of the APT10 backdoor, UPPERCUT.

Picture source: https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf

Infrastructure Tracking and Attribution



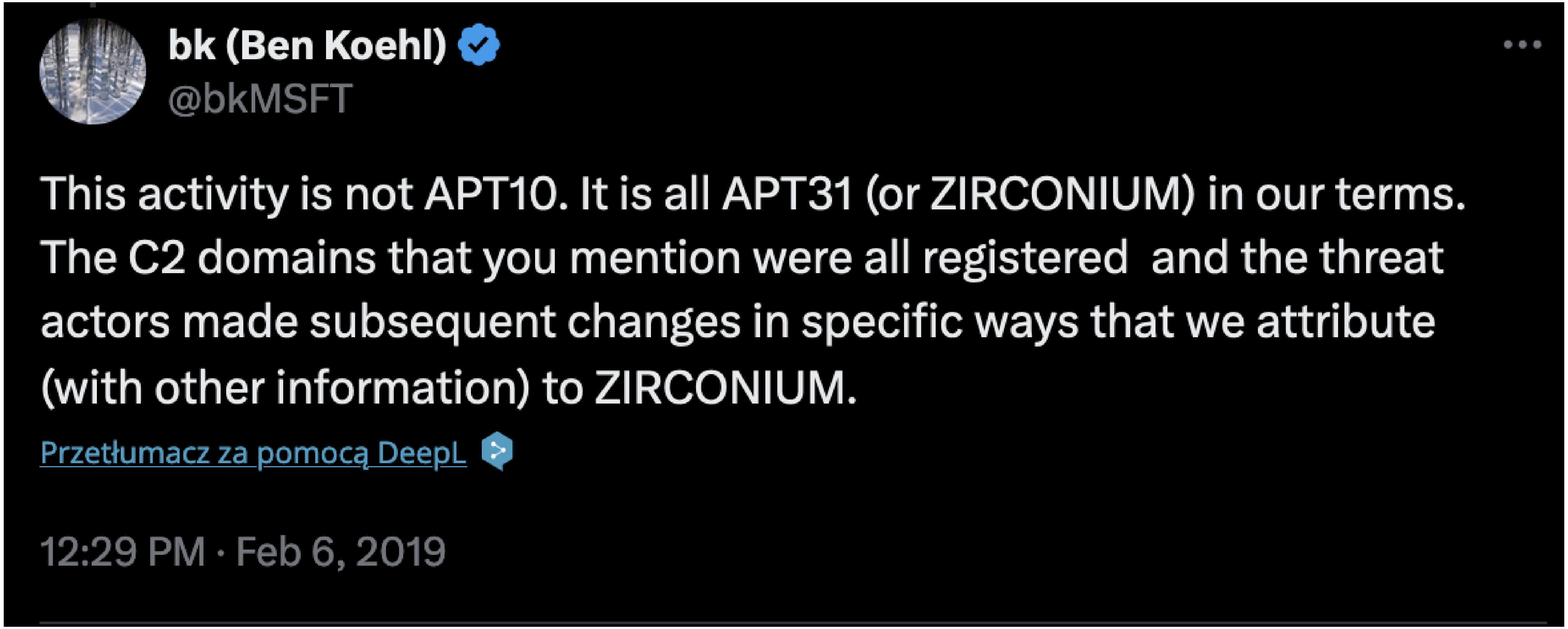
4. Extensive use of command-line tools including, but not limited to, Mimikatz, cURL for Windows, BITSAdmin, and WinRAR, to perform actions on-host.

5. The targeting of a Norwegian MSP, which enabled potential access to an extensive customer base. We believe that the APT10 targeting of Visma is an extension of their 2017 Cloud Hopper operation (which victimized some of the world's largest MSPs) and has continued into late 2018.

6. The unauthorized access to Citrix remote desktop clients at Visma using stolen credentials occured at times corresponding to Tianjin working hours (GMT +8).

Picture source: https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf

Infrastructure Tracking and Attribution



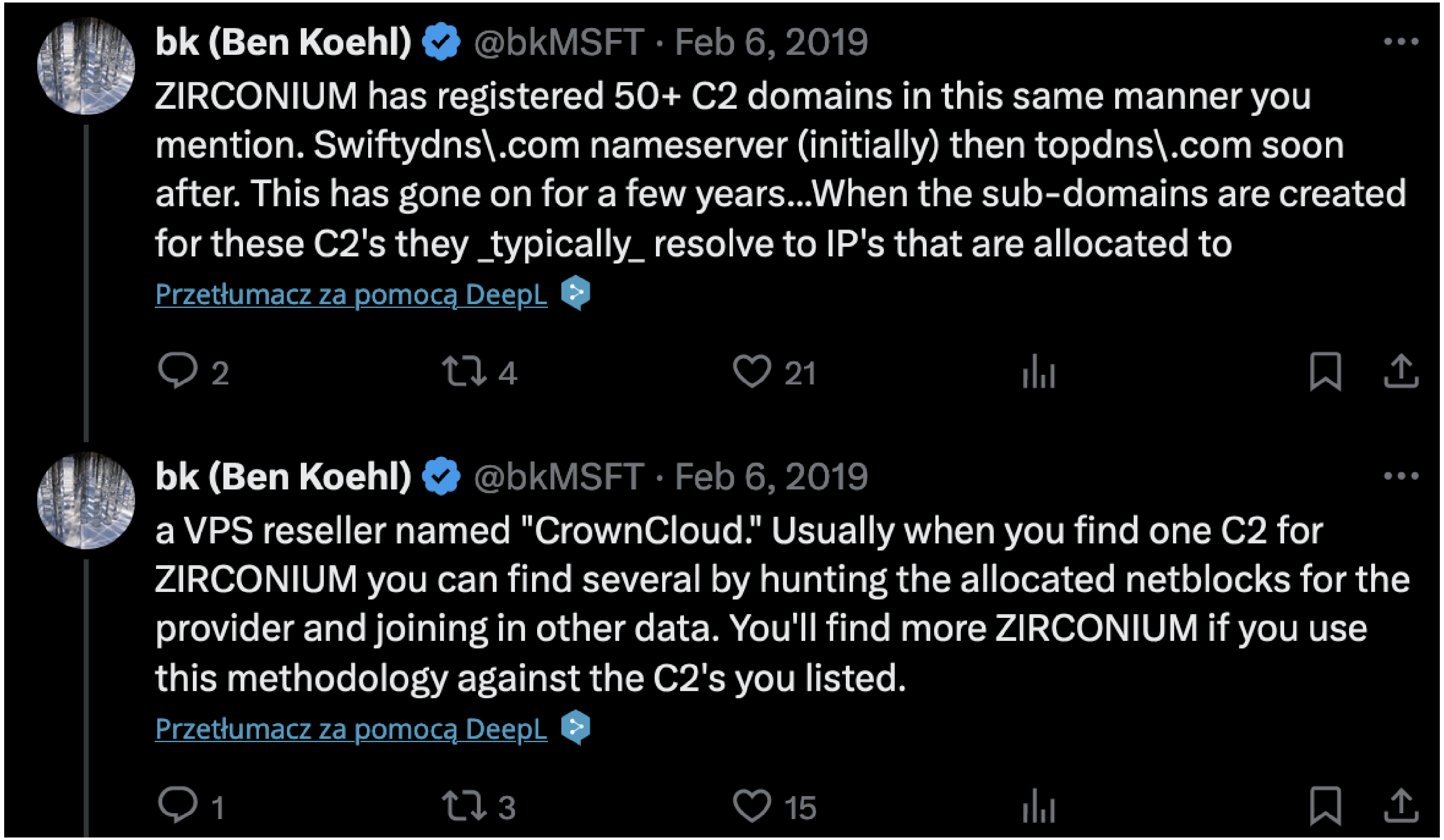
bk (Ben Koehl)
@bkMSFT

This activity is not APT10. It is all APT31 (or ZIRCONIUM) in our terms. The C2 domains that you mention were all registered and the threat actors made subsequent changes in specific ways that we attribute (with other information) to ZIRCONIUM.

Przetłumacz za pomocą DeepL

12:29 PM · Feb 6, 2019

Infrastructure Tracking and Attribution



bk (Ben Koehl) @bkMSFT · Feb 6, 2019

ZIRCONIUM has registered 50+ C2 domains in this same manner you mention. Swiftydns\.com nameserver (initially) then topdns\.com soon after. This has gone on for a few years...When the sub-domains are created for these C2's they _typically_ resolve to IP's that are allocated to

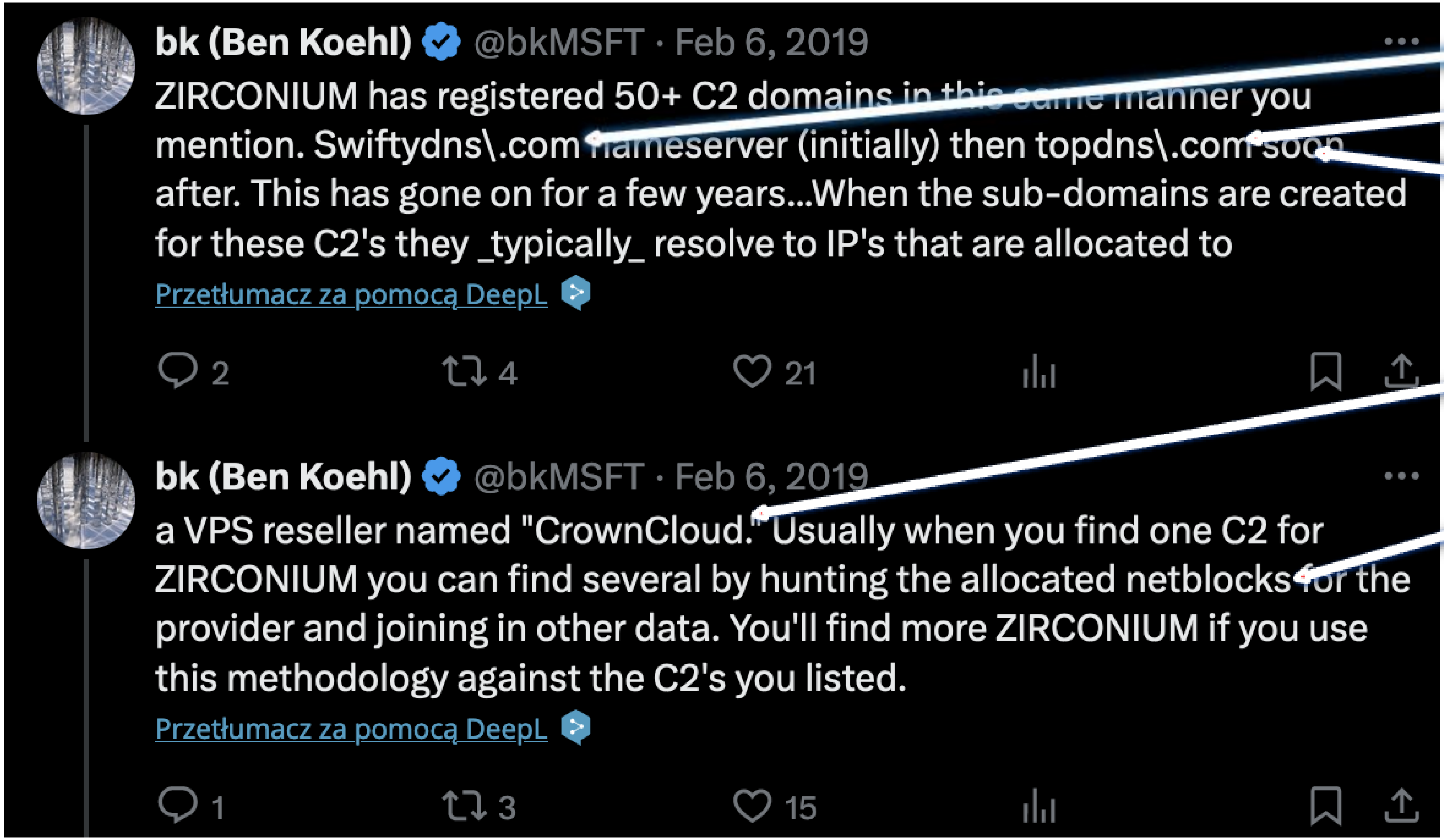
Przetłumacz za pomocą DeepL

bk (Ben Koehl) @bkMSFT · Feb 6, 2019

a VPS reseller named "CrownCloud." Usually when you find one C2 for ZIRCONIUM you can find several by hunting the allocated netblocks for the provider and joining in other data. You'll find more ZIRCONIUM if you use this methodology against the C2's you listed.

Przetłumacz za pomocą DeepL

Infrastructure Tracking and Attribution



bk (Ben Koehl) @bkMSFT · Feb 6, 2019

ZIRCONIUM has registered 50+ C2 domains in this same manner you mention. Swiftydns\.com nameserver (initially) then topdns\.com soon after. This has gone on for a few years...When the sub-domains are created for these C2's they _typically_ resolve to IP's that are allocated to

Przetłumacz za pomocą DeepL

2 4 21

bk (Ben Koehl) @bkMSFT · Feb 6, 2019

a VPS reseller named "CrownCloud." Usually when you find one C2 for ZIRCONIUM you can find several by hunting the allocated netblocks for the provider and joining in other data. You'll find more ZIRCONIUM if you use this methodology against the C2's you listed.

Przetłumacz za pomocą DeepL

1 3 15

Nameservers

Temporal pattern

Hosting provider

IP ranges

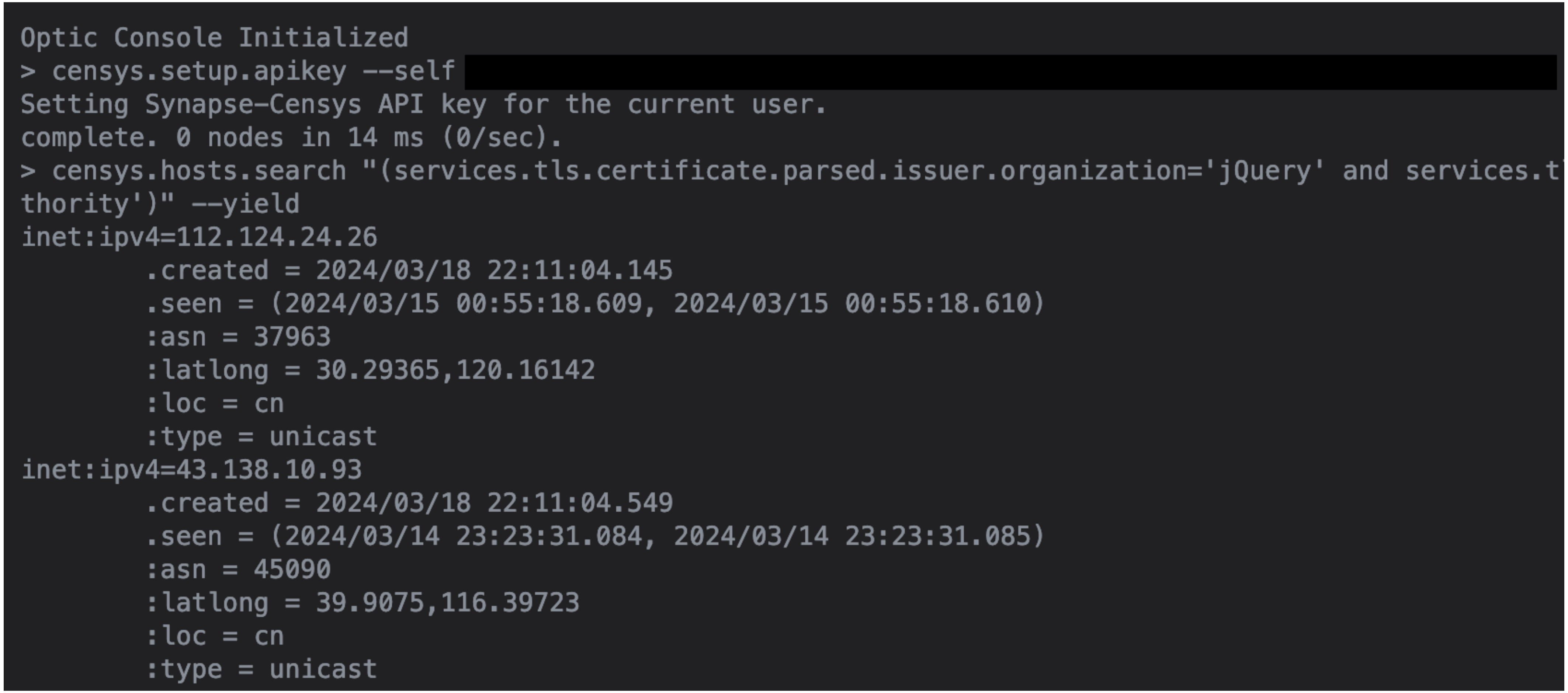
Indicator Sharing For Effective Defense

Picture source: https://imgflip.com/memegenerator/197671929/Kombucha-Girl

Indicator Sharing For Effective Defense

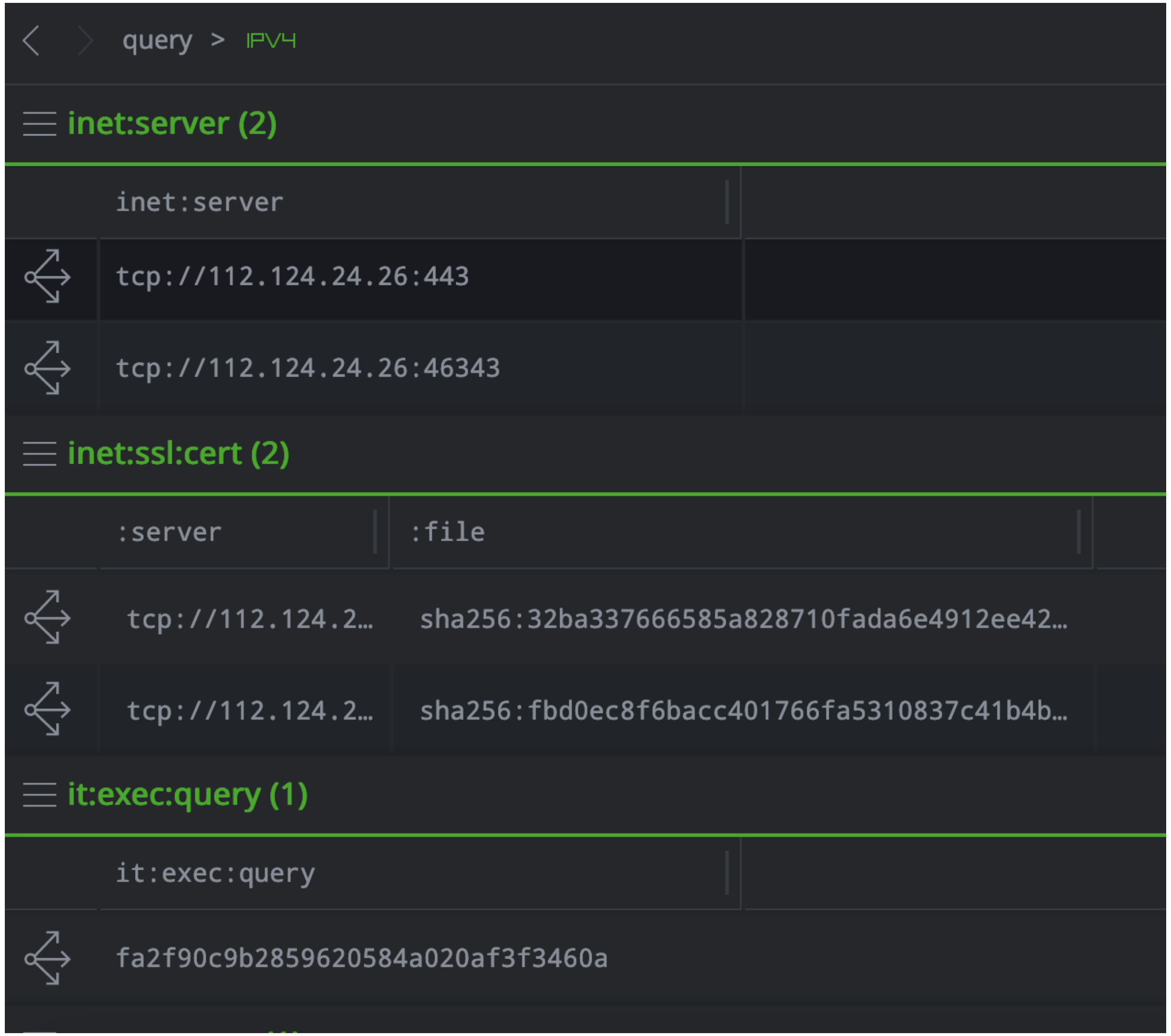
HUNTING AND TRACKING ADVERSARIES
co-authored by Pasquale Stirparo
#SynapseOrItDidNotHappen
presented by Bartek Jerzman
2023 FIRST Cyber Threat Intelligence Conference
#FIRSTCTI23
SPEAKER
Berlin, Germany
November 6-8, 20
www.first.org/conference/berlin2023

Indicator Sharing For Effective Defense



```
Optic Console Initialized
> censys.setup.apikey --self [redacted]
Setting Synapse-Censys API key for the current user.
complete. 0 nodes in 14 ms (0/sec).
> censys.hosts.search "(services.tls.certificate.parsed.issuer.organization='jQuery' and services.t
thority')" --yield
inet:ipv4=112.124.24.26
        .created = 2024/03/18 22:11:04.145
        .seen = (2024/03/15 00:55:18.609, 2024/03/15 00:55:18.610)
        :asn = 37963
        :latlong = 30.29365,120.16142
        :loc = cn
        :type = unicast
inet:ipv4=43.138.10.93
        .created = 2024/03/18 22:11:04.549
        .seen = (2024/03/14 23:23:31.084, 2024/03/14 23:23:31.085)
        :asn = 45090
        :latlong = 39.9075,116.39723
        :loc = cn
        :type = unicast
```

Indicator Sharing For Effective Defense



inet:server (2)

inet:server
tcp://112.124.24.26:443
tcp://112.124.24.26:46343

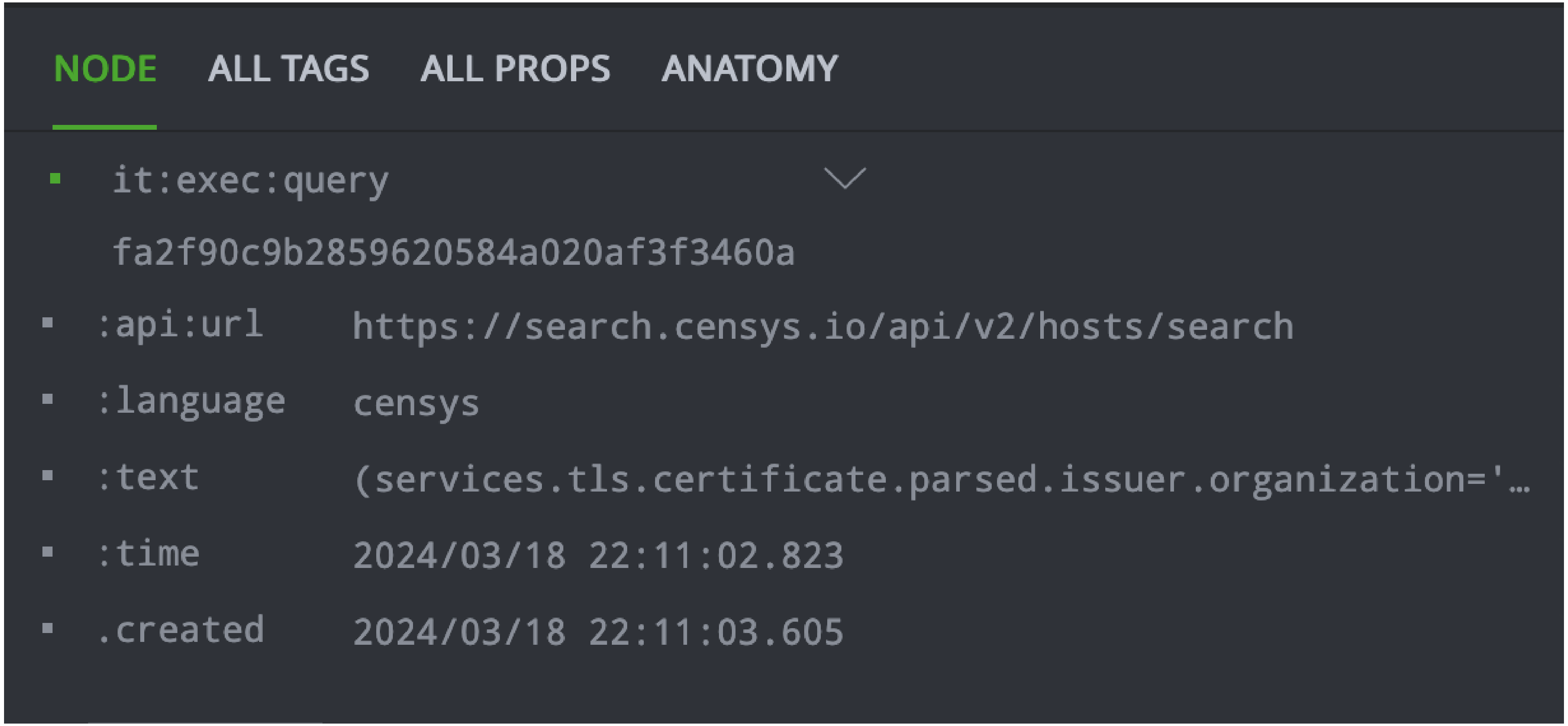
inet:ssl:cert (2)

:server	:file
tcp://112.124.2…	sha256:32ba337666585a828710fada6e4912ee42…
tcp://112.124.2…	sha256:fbd0ec8f6bacc401766fa5310837c41b4b…

it:exec:query (1)

it:exec:query
fa2f90c9b2859620584a020af3f3460a

Indicator Sharing For Effective Defense



```
▪ it:exec:query
  fa2f90c9b2859620584a020af3f3460a
▪ :api:url     https://search.censys.io/api/v2/hosts/search
▪ :language    censys
▪ :text        (services.tls.certificate.parsed.issuer.organization='…
▪ :time        2024/03/18 22:11:02.823
▪ .created     2024/03/18 22:11:03.605
```

2024
FIRST
Cyber Threat Intelligence Conference

Berlin, Germany
April 15-17, 2024

Thank you!