Infrastructure Hunting Challenge Coin

Please sign-up for the below accounts use a personal or work email

Shodan – www.shodan.io
Virustotal – www.virustotal.com
URLScan – www.urlscan.io

Bridewell

Bridewell

Cyber Security.
Where it Matters.

Malicious Infrastructure Tracking CTF

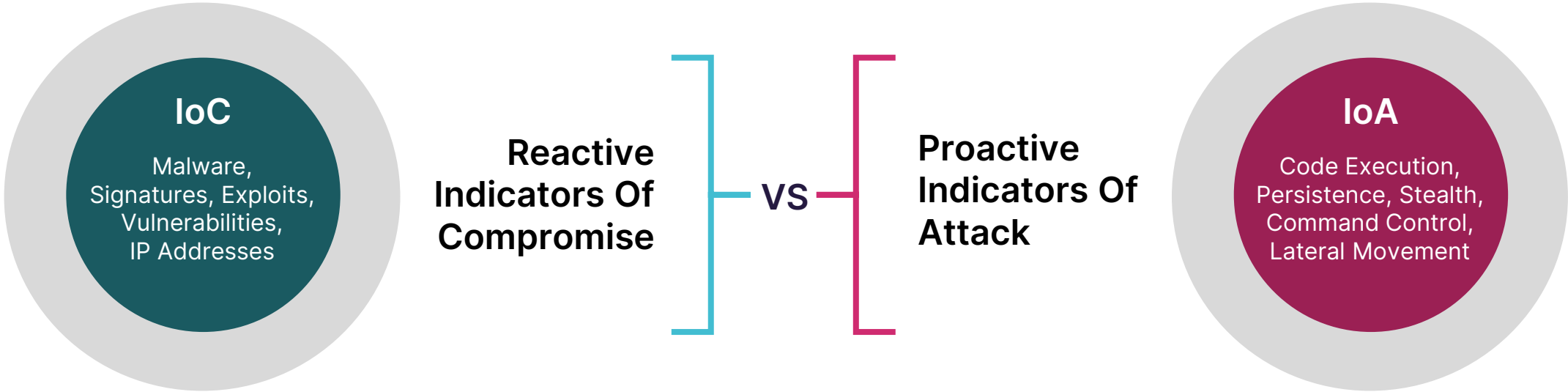
Indicators of Attack (IoA)

Current Industry Standard

Indicators of Compromise (IoC) resulting from incidents and identifying patterns of malicious activity, which is often reactive and only detects C&C infrastructure known to be malicious.

Bridewell CTI Approach

This proactive approach is more effective at identifying emerging threats known as Indicators of Attack (IoA) and allows for faster responses to security breaches.

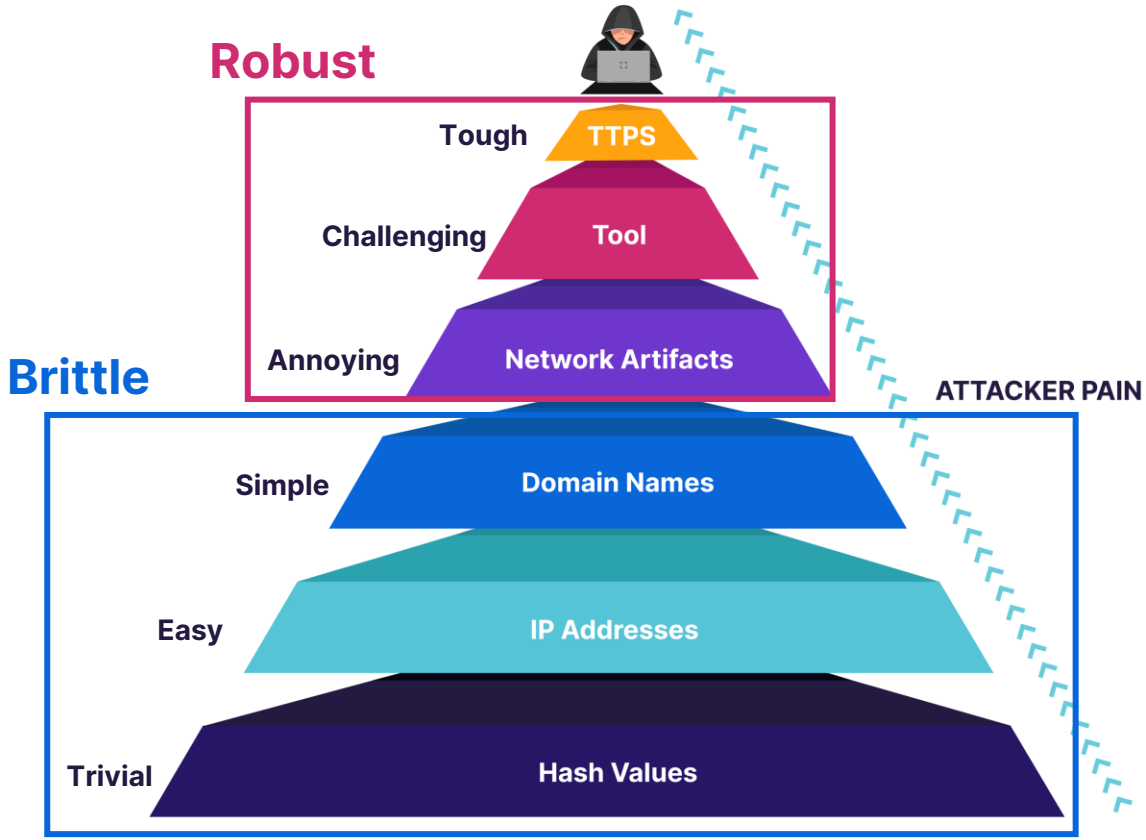


Detection Robustness

Payloads, files, infrastructure and tools can be replaced, with an increasing degree of difficulties, but human behavior is difficult to change.

The “Pyramid of Pain”, developed in 2013 by David J Bianco is a key conceptual model for the effective use of Cyber Threat Intelligence within Cyber Security.

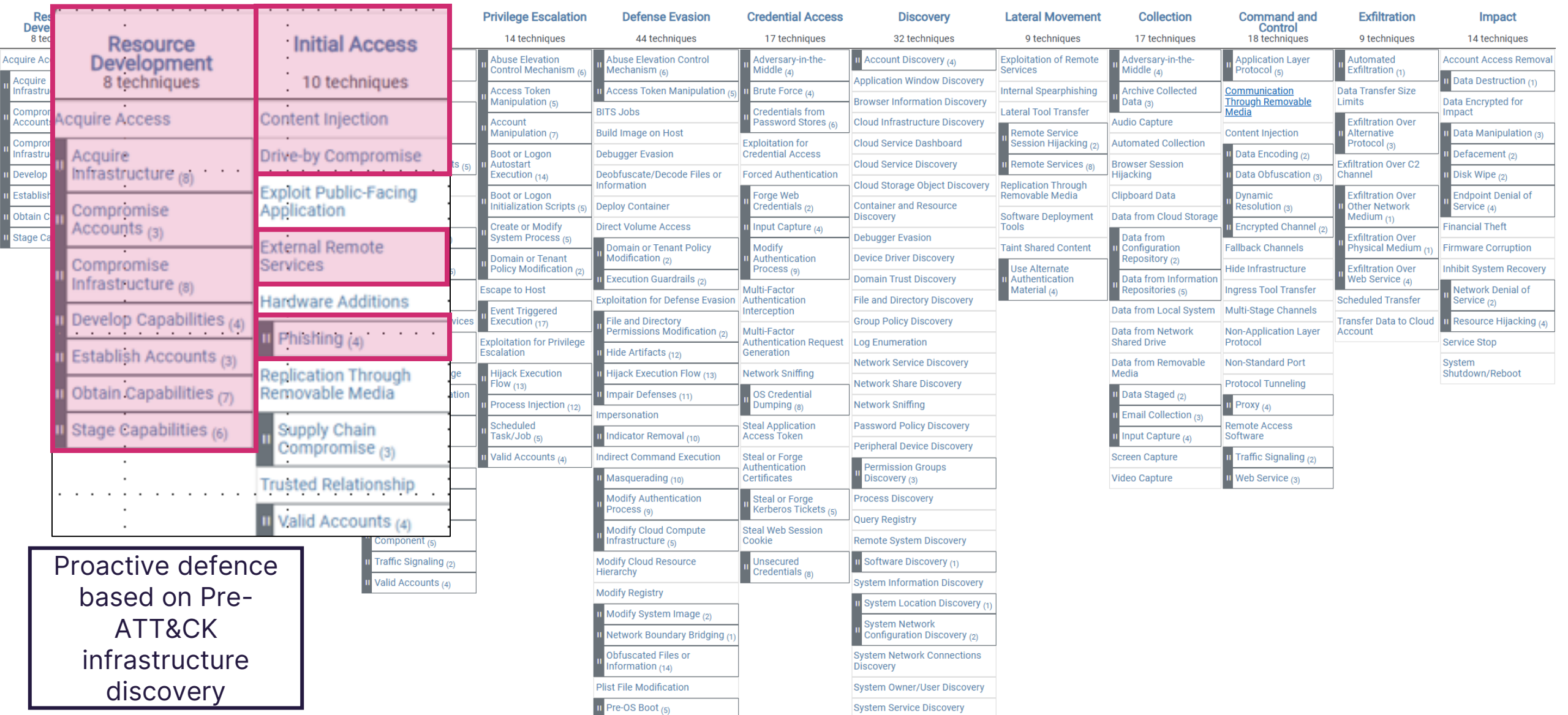
- **At the bottom of the pyramid are the elements that can easily be changed, with very little annoyance to a threat actor.**
- **Threat intelligence can prioritise indicators at the top of the pyramid to ensure detection is robust.**
- **Indicators of Attack (IoA) are harder for the adversary to change and often persist for longer.**



Threat Actor Disruption Through Research

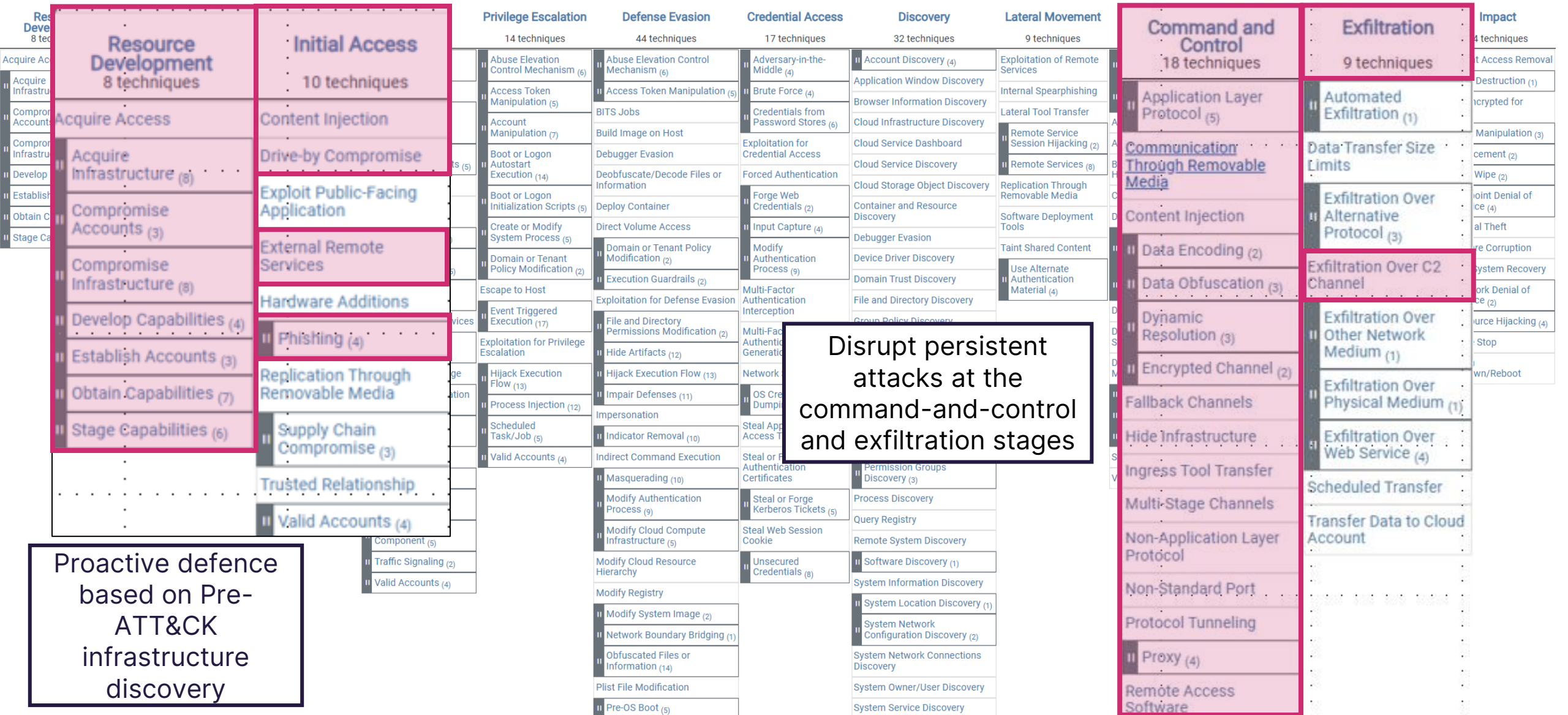
THREAT ACTORS HAVE OPTIONS ;)

Threat Actor Disruption Through Research

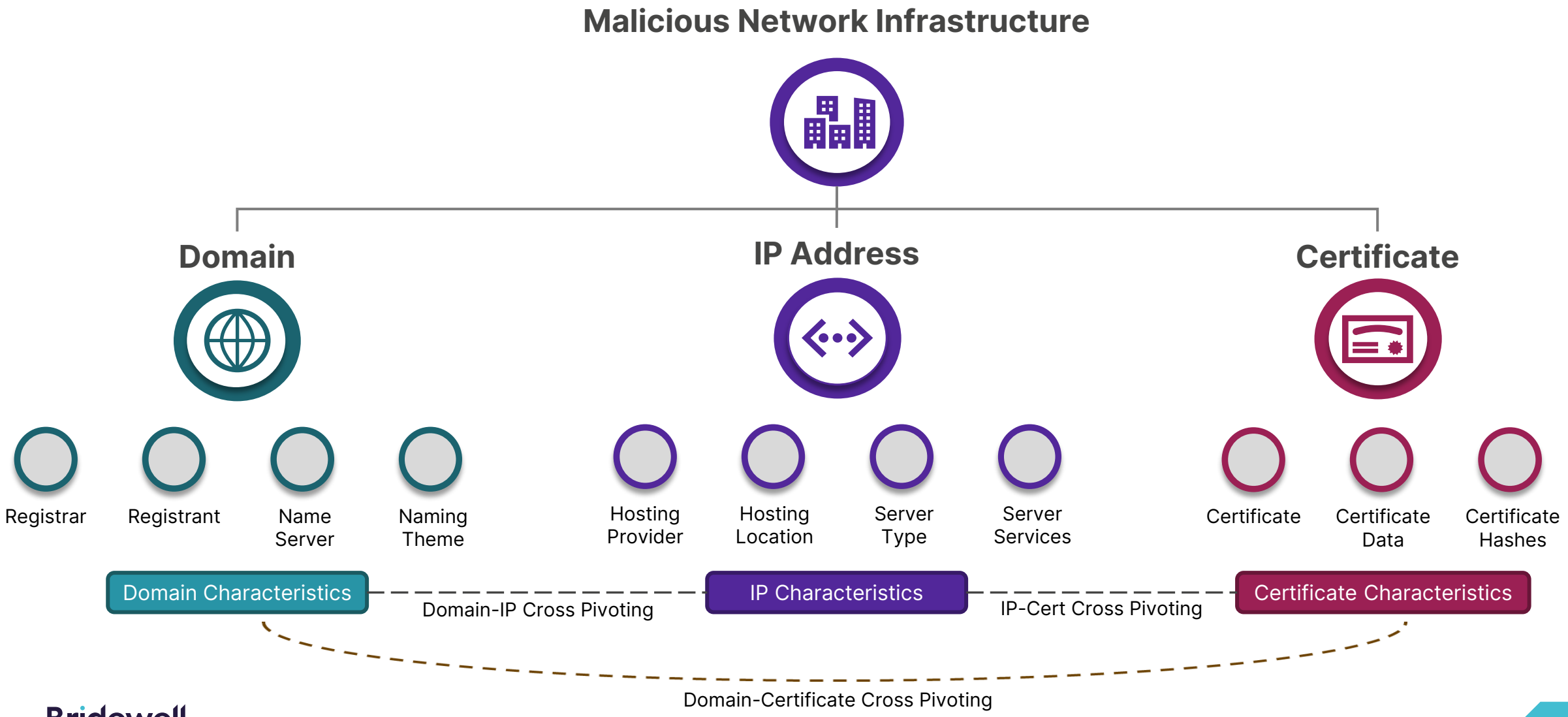


Proactive defence based on Pre-ATT&CK infrastructure discovery

Threat Actor Disruption Through Research



Malicious Infrastructure Pivots



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

Tools

urlscan.io
A sandbox for the web

Bridewell

Infrastructure Hunting Examples

Cyber Consulting

Managed Security

Penetration Testing

Data Privacy

Cybercrime – RATs

Overview

AsyncRAT is an open-source Remote Access Trojan (RAT) designed for stealthy remote administration of compromised systems. It allows attackers to persist on infected machines, exfiltrate data, and execute commands through an encrypted C2 connection. It is used by threat actors, including cybercriminals and APT groups, to facilitate espionage, ransomware deployment, and credential theft.

Key Capabilities

- Remote Control
- Stealth & Persistence
- Keylogging & Credential Theft
- Encrypted C2 Communication
- Clipboard Hijacking

Bridewell

Cybercrime – RATs

AsyncRAT

The AsyncRAT default configuration contains a fingerprint within the SSL certificates that can be used to profile the C2.

TOTAL RESULTS

49

TOP COUNTRIES

Netherlands	18
United States	11
Poland	5
Germany	4
France	3

More...

TOP PORTS

4444	12
444	9

View Report | Download Results | H

Product Spotlight: We've Launched a new

45.154.98.68

45.154.98.68.powered.by.rdp.sh

1337 Services GmbH

Netherlands, Lelystad

c2 self-signed

SSL Certificate

Issued By:

|- Common Name:

AsyncRAT Server

Issued To:

|- Common Name:

AsyncRAT Server

Supported SSL Versions:

TLSv1

45.138.16.236

1337 Services GmbH

Poland, Warsaw

c2 self-signed

SSL Certificate

Issued By:

|- Common Name:

AsyncRAT Server

Issued To:

|- Common Name:

AsyncRAT Server

Supported SSL Versions:

TLSv1

Cybercrime – RATs

Shodan rule:
ssl:"AsyncRAT Server"

SHODAN ssl:"AsyncRAT Server"

TOTAL RESULTS

49

TOP COUNTRIES

Netherlands	18
United States	11
Poland	5
Germany	4
France	3

More...

TOP PORTS

4444	12
444	9

Product Spotlight: We've Launched a new

45.154.98.68
45.154.98.68.powered.by.rdp.sh
1337 Services GmbH
Netherlands, Lelystad

c2 self-signed

SSL Certificate
Issued By:
|- Common Name:
AsyncRAT Server
Issued To:
|- Common Name:
AsyncRAT Server
Supported SSL Versions:
TLSv1

45.138.16.236
1337 Services GmbH
Poland, Warsaw

c2 self-signed

SSL Certificate
Issued By:
|- Common Name:
AsyncRAT Server
Issued To:
|- Common Name:
AsyncRAT Server
Supported SSL Versions:
TLSv1

Cybercrime – Offensive Security Tools (OST)

Overview

Offensive security tools (OST), originally developed for legitimate purposes such as penetration testing and red teaming, are increasingly being misused by various threat actors including both Cybercriminals and Nation-state actors.

Cobalt Strike: A red-team tool repurposed by threat actors for stealthy C2, payload delivery, and lateral movement.

Sliver: An open-source C2 framework with modular implants, multiple C2 channels, and strong evasion tactics.

Metasploit: A penetration testing framework used for exploitation, privilege escalation, and payload deployment.

Bridewell

Cybercrime – Offensive Security Tools (OST)

SHODAN ssl.cert.subject.cn:"multiplayer" ssl.cert.issuer.cn:"operators"

Sliver

There are numerous Sliver servers deployed globally some using default configurations.

One way we have consistently tracked Sliver is by combining both server and certificate characteristics such as SSL JARM, HTTP header content etc.

194.233.73.173

vmi1243780.contabo server.net

Contabo Asia Private Limited

Singapore, Singapore

SSL Certificate

Issued By:
|- Common Name:
operators

Issued To:
|- Common Name:
multiplayer

SSL Error: TLSV1_ALERT_PROTOCOL_VERSION

8.210.236.220

Alibaba Cloud (Singapore) Private Limited

Hong Kong, Hong Kong

cloud

SSL Certificate

Issued By:
|- Common Name:
operators

Issued To:
|- Common Name:
multiplayer

SSL Error: TLSV1_ALERT_PROTOCOL_VERSION

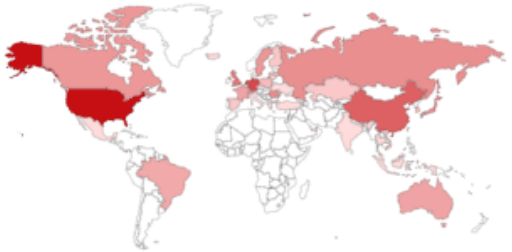
Hunt Rules:
ssl.cert.subject.cn:"multiplayer" ssl.cert.issuer.cn:"operators“

ssl:”multiplayer” ssl:”operators”

TOTAL RESULTS

430

TOP COUNTRIES



United States	110
Germany	43
Hong Kong	43
Netherlands	41
China	27

More...

TOP PORTS

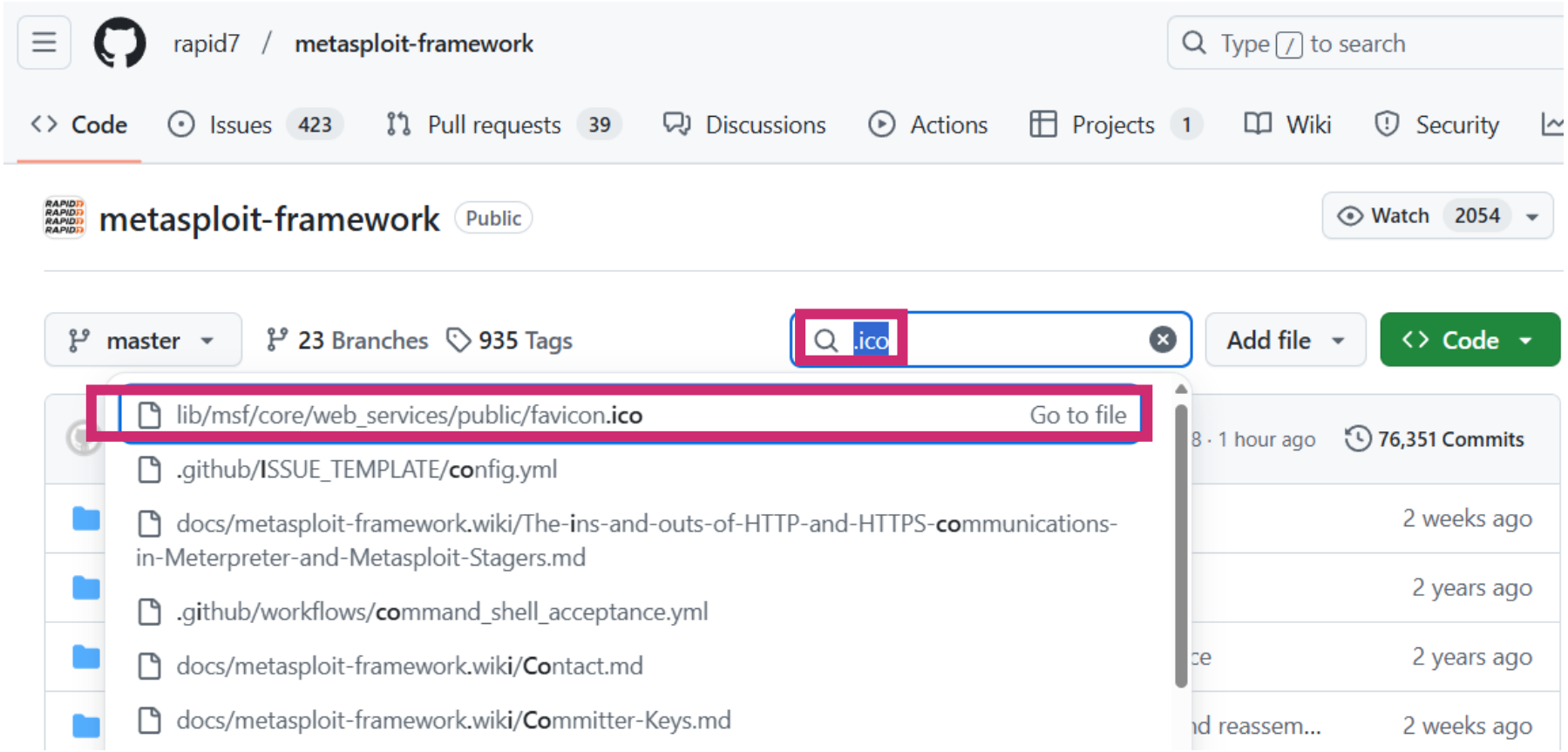
31337	427
8443	2

Cybercrime – Offensive Security Tools (OST)

Metasploit

There are a couple of options to track the default Metasploit configuration.

It is possible to leverage both the Favicon hash and certificate information to track these servers.

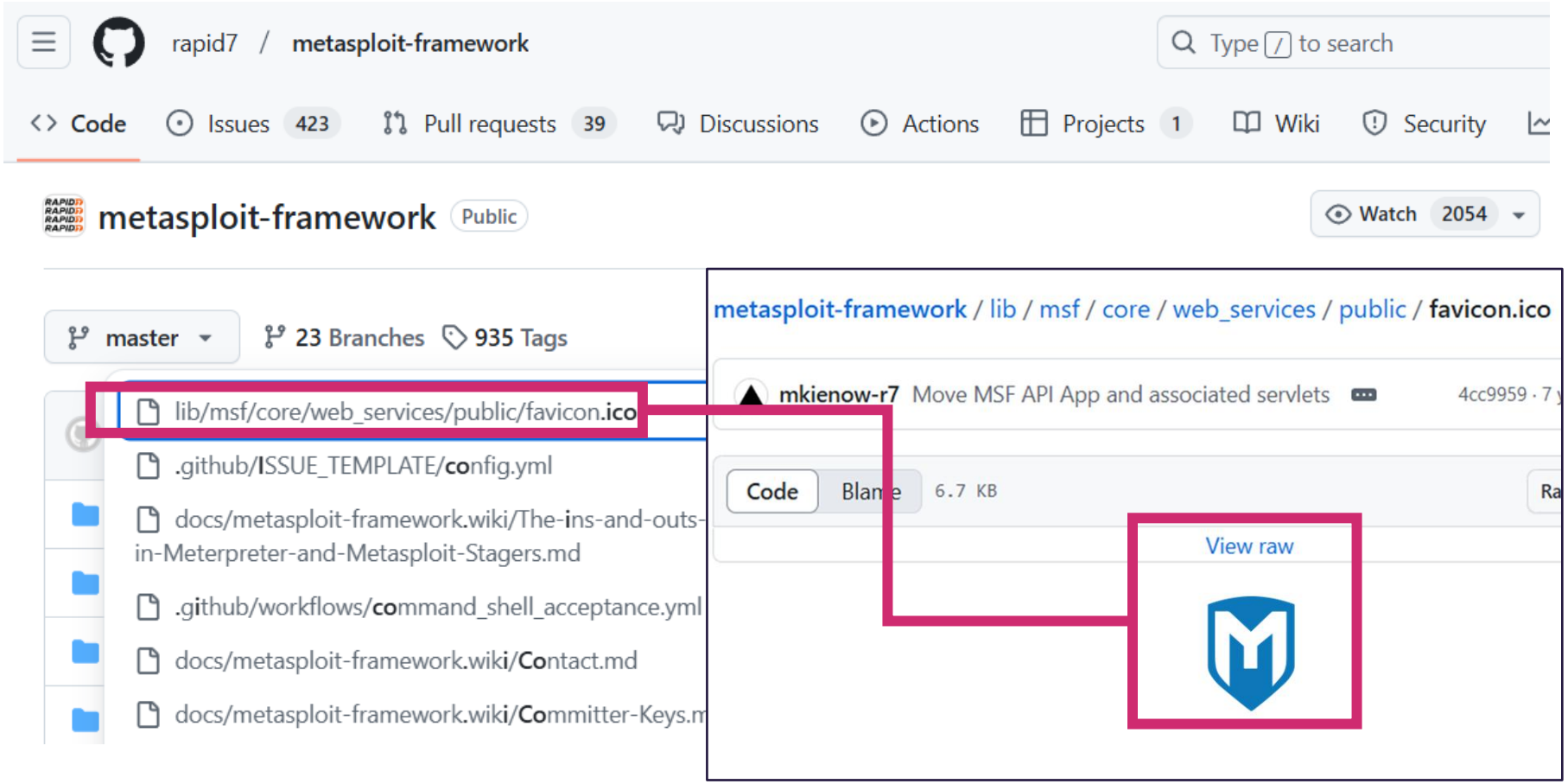


Cybercrime – Offensive Security Tools (OST)

Metasploit

By using the public GitHub repository, we can search for a favicon icon to understand whether this could be used to track the server.

The hash of the favicon can then be used to search in tools like Shodan for websites that may also have the same favicon.



Cybercrime – Offensive Security Tools (OST)

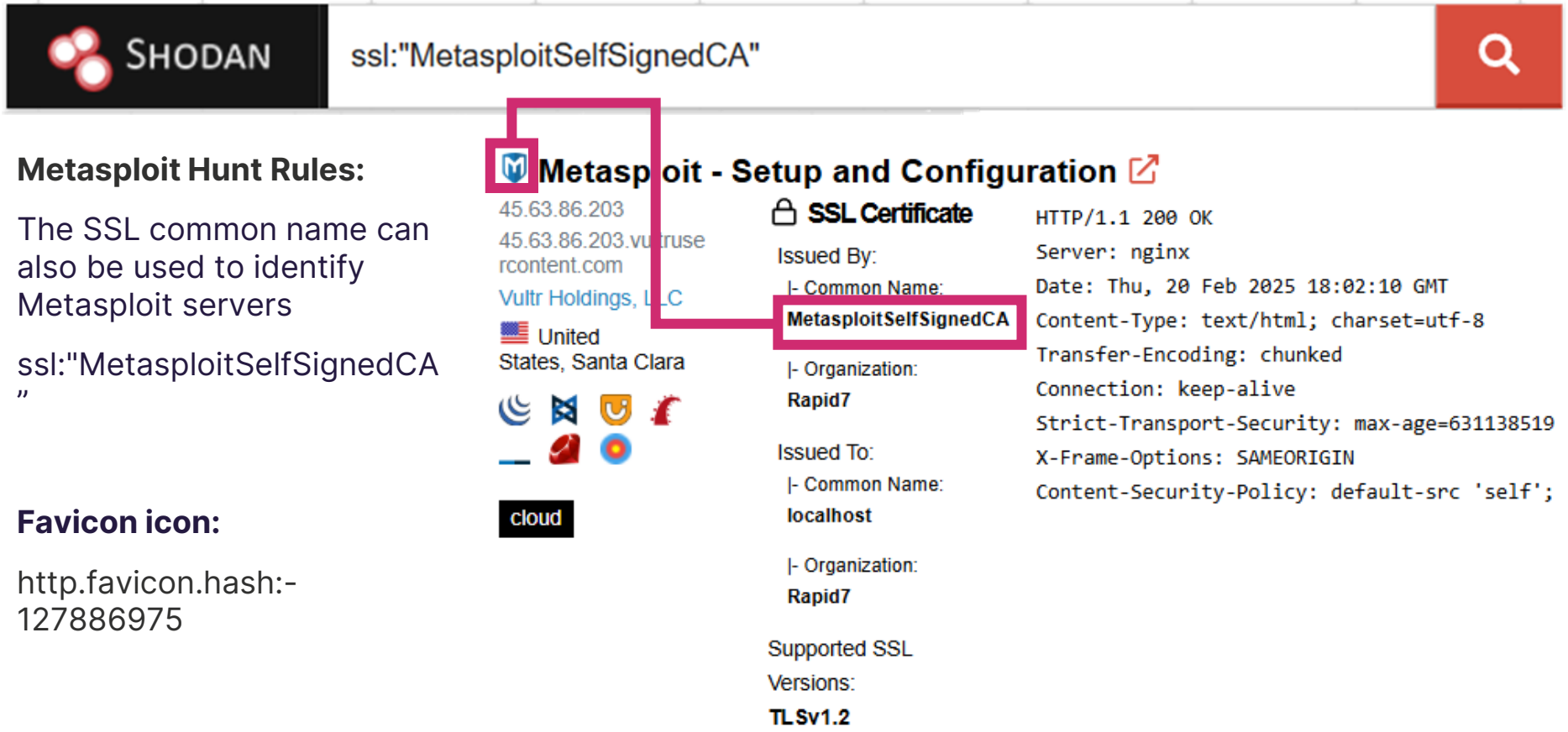
Metasploit Hunt Rules:

The SSL common name can also be used to identify Metasploit servers

ssl:"MetasploitSelfSignedCA"

Favicon icon:

http.favicon.hash:-127886975



TOTAL RESULTS

313

TOP COUNTRIES

United States	76
Germany	51
Hong Kong	23
France	18
United Kingdom	18

More...

TOP PORTS

3790	311
3780	1

Cybercrime – Offensive Security Tools (OST)

Cobalt Strike

There are numerous Cobalt Strike servers deployed globally some using default, and others with custom configurations.

One way we have consistently tracked Cobalt Strike is by combining both server and certificate characteristics such as SSL JARM, HTTP header content etc.

118.31.0.235

Aliyun Computing Co., LTD

China, Hangzhou

self-signed

2025-09-04T06:21:14.080768

SSL Certificate

Issued By:
- |- Common Name:
- |- Organization:

Issued To:
- |- Common Name:
- |- Organization:

Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 404 Not Found
Date: Thu, 4 Sep 2025 06:21:13 GMT
Content-Type: text/plain
Content-Length: 0

Cobalt Strike Beacon:
  x86:
    beacon_type: HTTPS
    cfg_caution: 1
    dns-beacon.strategy_fail_seconds: -1
    dns-beacon.strategy_fail_x: -1
    dns-beacon.strategy_rotate_seconds: -1...
```

8.148.194.157

Aliyun Computing Co.LTD

China, Guangzhou

cloud self-signed

2025-09-04T05:48:34.447978

SSL Certificate

Issued By:
- |- Common Name: **jquery.com**
- |- Organization: **jQuery**

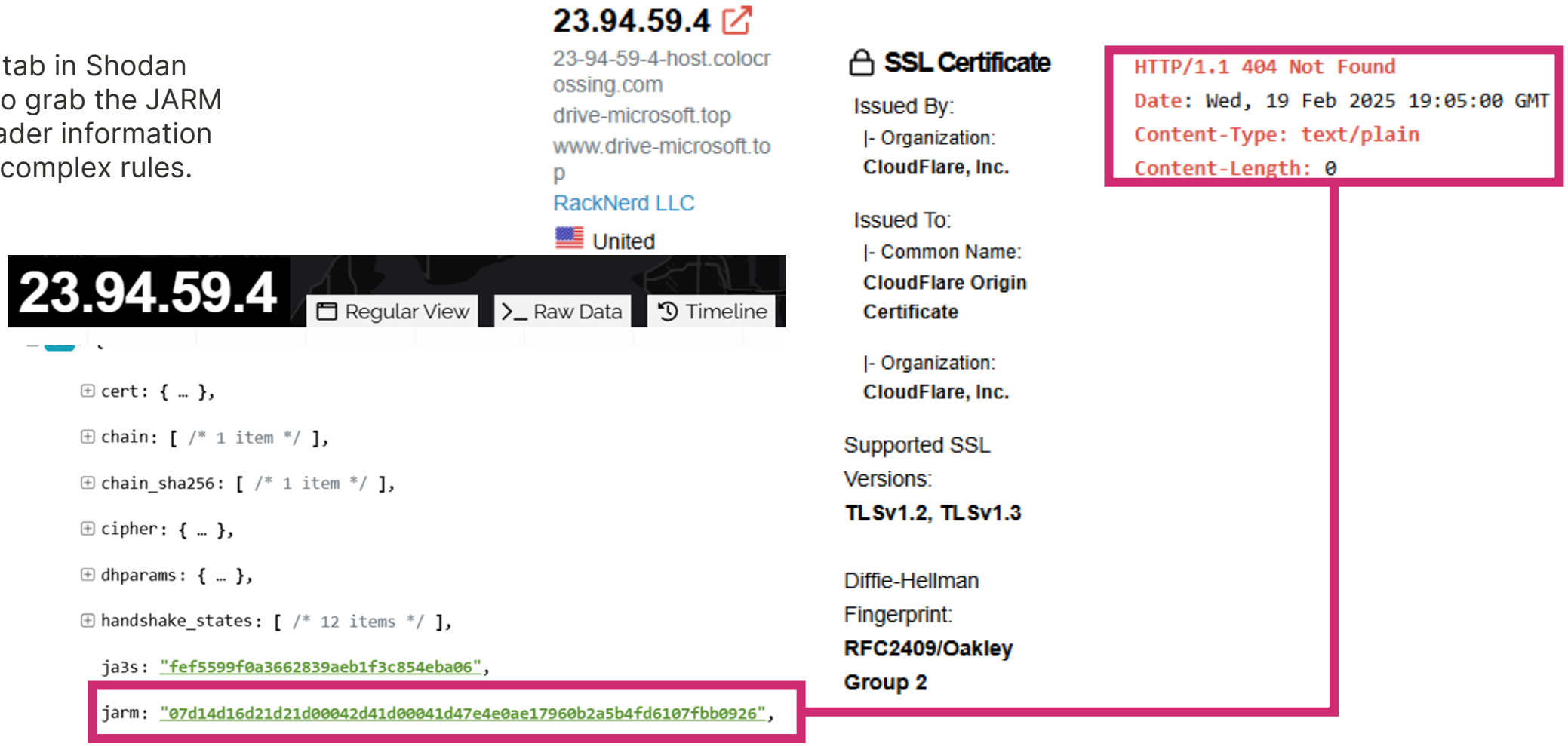
Issued To:
- |- Common Name:

```
HTTP/1.1 404 Not Found
Date: Thu, 4 Sep 2025 05:48:34 GMT
Server: Apache
Content-Length: 0
Keep-Alive: timeout=10, max=100
Connection: Keep-Alive
Content-Type: text/plain
```

Cybercrime – Offensive Security Tools (OST)

Cobalt Strike

The raw data tab in Shodan can be used to grab the JARM and HTTP header information to form more complex rules.



Bridewell

Infrastructure Hunting Challenge

Cyber Consulting

Managed Security

Penetration Testing

Data Privacy

Mission Briefing: Operation Shadow Trace (Hunt. Expose. Defend.)

You are part of **Sentinel Security Research**, an **elite cyber intelligence unit** tasked with tracking and exposing the **world's most dangerous threat actors.**

Your Mission

The UK's Critical National Infrastructure (CNI) is under attack. Use OSINT sources to **uncover adversary-controlled infrastructure**. Correlate data to reveal hidden threat actor footprints. Map out malicious infrastructure before the next attack occurs.

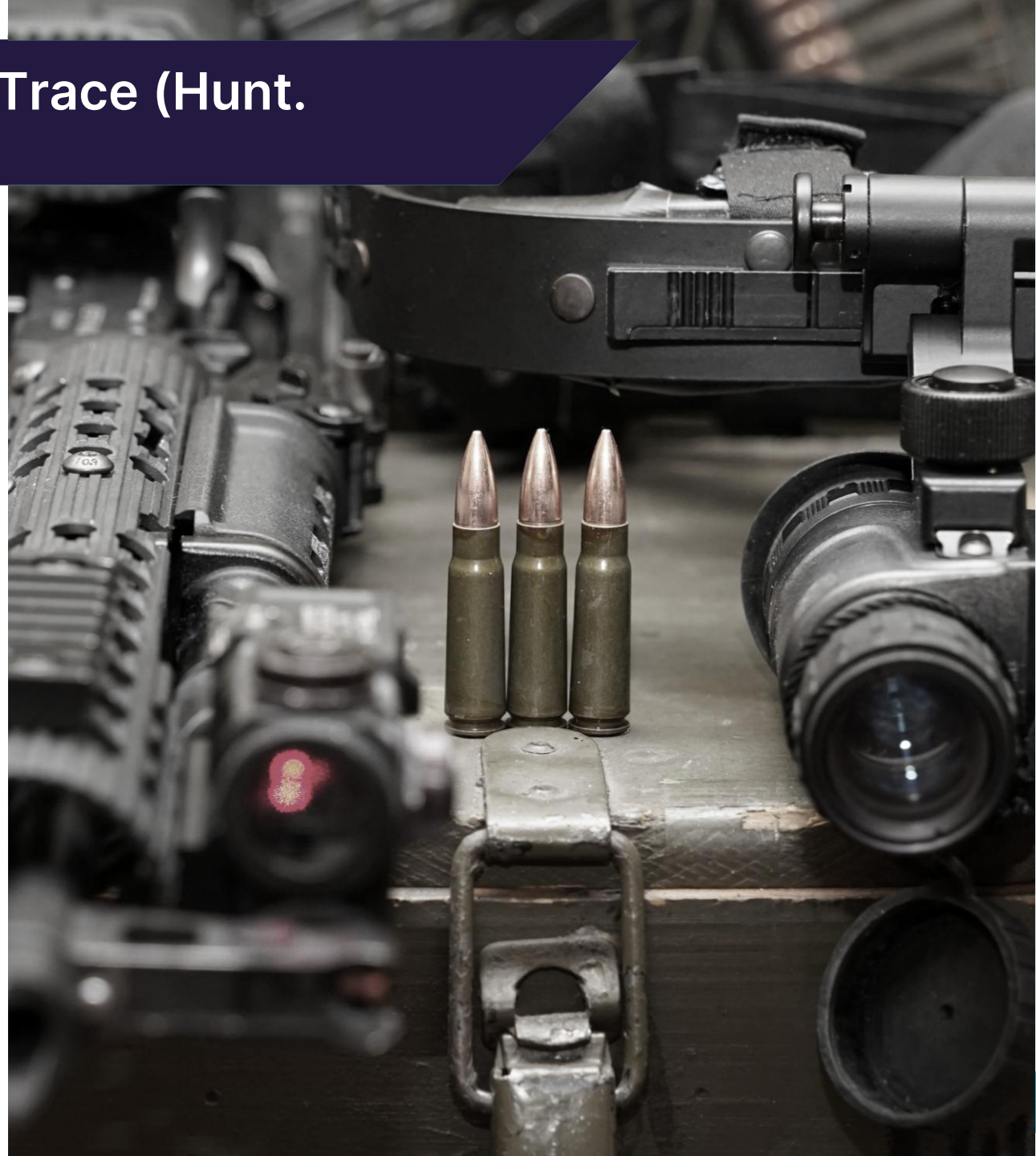
Your Tools:

URLscan.io, Shodan.io, Virustotal.com, Abuse.ch, Google ☺

The Reward

The top-performing analysts will **win an exclusive Challenge Coin** a symbol of cyber threat hunting excellence.

The clock is ticking. The future of UK CNI depends on you. Get ready. Gear up. Hunt the adversary !!!



Bridewell

Logging In

Use your table number for username and password:

E.G.
Username = table1
Password = table1

https://cni-ctf.com/login

Please sign-up and use the below tools to solve questions:

Shodan – www.shodan.io
Virustotal – www.virustotal.com
URLScan – www.urlscan.io

Bridewell

Cyber Security.
Where it Matters.

Find out how Bridewell can transform and protect your organisation's critical business functions through our modern cyber security services.

+44 (0)3308 285 880

josh.penny@bridewell.com, gavin.knapp@bridewell.com

www.bridewell.com