

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

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.



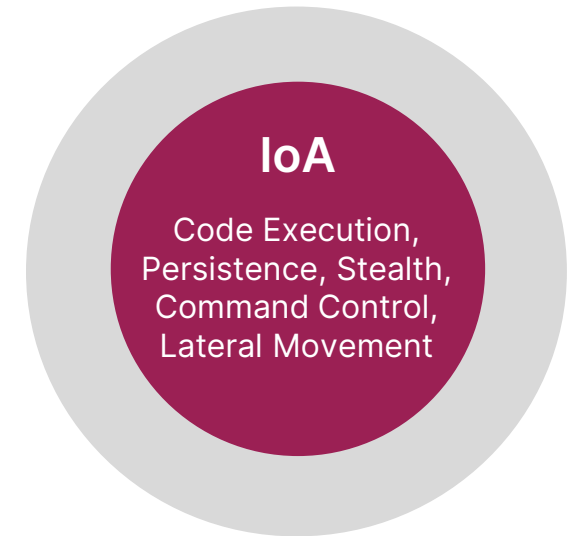
**Reactive
Indicators Of
Compromise**

VS

**Proactive
Indicators Of
Attack**

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.

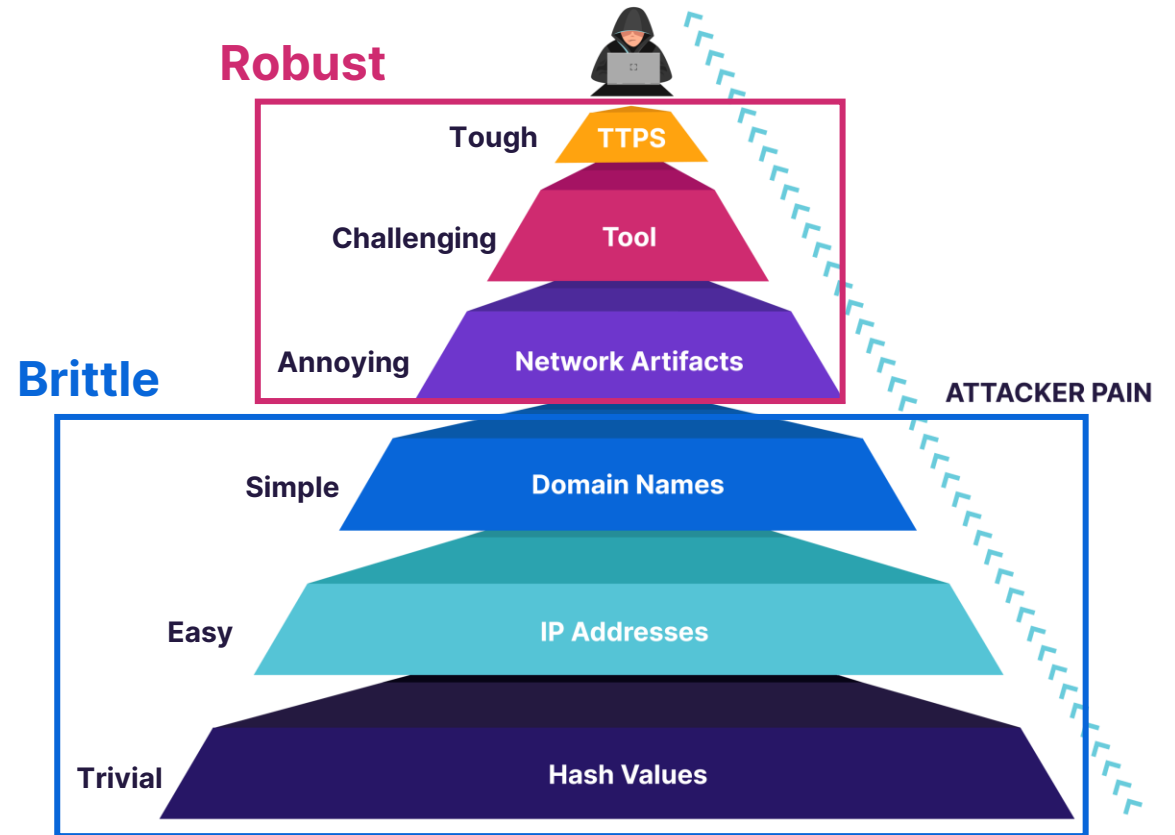


Detection Robustness

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

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 44 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
<div> <div>Active Scanning (3)</div> <div>Gather Victim Host Information (4)</div> <div>Gather Victim Identity Information (3)</div> <div>Gather Victim Network Information (6)</div> <div>Gather Victim Org Information (4)</div> <div>Phishing for Information (4)</div> <div>Search Closed Sources (2)</div> <div>Search Open Technical Databases (5)</div> <div>Search Open Websites/Domains (3)</div> <div>Search Victim-Owned Websites</div> </div>	<div> <div>Acquire Access</div> <div>Acquire Infrastructure (8)</div> <div>Compromise Accounts (3)</div> <div>Compromise Infrastructure (8)</div> <div>Develop Capabilities (4)</div> <div>Establish Accounts (3)</div> <div>Obtain Capabilities (7)</div> <div>Stage Capabilities (6)</div> </div>	<div> <div>Content Injection</div> <div>Drive-by Compromise</div> <div>Exploit Public-Facing Application</div> <div>External Remote Services</div> <div>Hardware Additions</div> <div>Phishing (4)</div> <div>Replication Through Removable Media</div> <div>Supply Chain Compromise (3)</div> <div>Trusted Relationship</div> <div>Valid Accounts (4)</div> </div>	<div> <div>Cloud Administration Command</div> <div>Command and Scripting Interpreter (11)</div> <div>Container Administration Command</div> <div>Deploy Container</div> <div>Exploitation for Client Execution</div> <div>Inter-Process Communication (3)</div> <div>Native API</div> <div>Scheduled Task/Job (5)</div> <div>Serverless Execution</div> <div>Shared Modules</div> <div>Software Deployment Tools</div> <div>System Services (2)</div> <div>User Execution (3)</div> <div>Windows Management Instrumentation</div> </div>	<div> <div>Account Manipulation (7)</div> <div>BITS Jobs</div> <div>Boot or Logon Autostart Execution (14)</div> <div>Boot or Logon Initialization Scripts (5)</div> <div>Browser Extensions</div> <div>Compromise Host Software Binary</div> <div>Create Account (3)</div> <div>Create or Modify System Process (5)</div> <div>Domain or Tenant Policy Modification (2)</div> <div>Event Triggered Execution (17)</div> <div>Event Triggered Execution (17)</div> <div>External Remote Services</div> <div>Hijack Execution Flow (13)</div> <div>Implant Internal Image</div> <div>Modify Authentication Process (9)</div> <div>Office Application Startup (6)</div> <div>Power Settings</div> <div>Pre-OS Boot (5)</div> <div>Scheduled Task/Job (5)</div> <div>Server Software</div> </div>	<div> <div>Abuse Elevation Control Mechanism (6)</div> <div>Access Token Manipulation (5)</div> <div>Account Manipulation (7)</div> <div>Boot or Logon Autostart Execution (14)</div> <div>Boot or Logon Initialization Scripts (5)</div> <div>Create or Modify System Process (5)</div> <div>Domain or Tenant Policy Modification (2)</div> <div>Execution Guardrails (2)</div> <div>File and Directory Permissions Modification (2)</div> <div>Hide Artifacts (12)</div> <div>Hijack Execution Flow (13)</div> <div>Impair Defenses (11)</div> <div>Impersonation</div> <div>Indicator Removal (10)</div> <div>Indirect Command Execution</div> <div>Masquerading (10)</div> <div>Modify Authentication Process (9)</div> <div>Modify Cloud Compute Infrastructure (5)</div> <div>Modify Cloud Resource Hierarchy</div> <div>Modify Registry</div> <div>Modify System Image (2)</div> <div>Network Boundary Bridging (1)</div> <div>Obfuscated Files or Information (14)</div> <div>Plist File Modification</div> <div>Pre-OS Boot (5)</div> <div>Process Injection (12)</div> <div>Reflective Code Loading</div> <div>Rogue Domain Controller</div> </div>	<div> <div>Abuse Elevation Control Mechanism (6)</div> <div>Access Token Manipulation (5)</div> <div>BITS Jobs</div> <div>Build Image on Host</div> <div>Debugger Evasion</div> <div>Deobfuscate/Decode Files or Information</div> <div>Deploy Container</div> <div>Direct Volume Access</div> <div>Domain or Tenant Policy Modification (2)</div> <div>Execution Guardrails (2)</div> <div>Exploitation for Defense Evasion</div> <div>File and Directory Permissions Modification (2)</div> <div>Hide Artifacts (12)</div> <div>Hijack Execution Flow (13)</div> <div>Impair Defenses (11)</div> <div>Impersonation</div> <div>Indicator Removal (10)</div> <div>Indirect Command Execution</div> <div>Masquerading (10)</div> <div>Modify Authentication Process (9)</div> <div>Modify Cloud Compute Infrastructure (5)</div> <div>Modify Cloud Resource Hierarchy</div> <div>Modify Registry</div> <div>Modify System Image (2)</div> <div>Network Boundary Bridging (1)</div> <div>Obfuscated Files or Information (14)</div> <div>Plist File Modification</div> <div>Pre-OS Boot (5)</div> <div>Process Injection (12)</div> <div>Reflective Code Loading</div> <div>Rogue Domain Controller</div> </div>	<div> <div>Adversary-in-the-Middle (4)</div> <div>Brute Force (4)</div> <div>Credentials from Password Stores (6)</div> <div>Exploitation for Credential Access</div> <div>Forced Authentication</div> <div>Forge Web Credentials (2)</div> <div>Input Capture (4)</div> <div>Modify Authentication Process (9)</div> <div>Multi-Factor Authentication Interception</div> <div>Multi-Factor Authentication Request Generation</div> <div>Network Sniffing</div> <div>OS Credential Dumping (8)</div> <div>Steal Application Access Token</div> <div>Steal or Forge Authentication Certificates</div> <div>Steal or Forge Kerberos Tickets (5)</div> <div>Steal Web Session Cookie</div> <div>Unsecured Credentials (8)</div> </div>	<div> <div>Account Discovery (4)</div> <div>Application Window Discovery</div> <div>Browser Information Discovery</div> <div>Cloud Infrastructure Discovery</div> <div>Cloud Service Dashboard</div> <div>Cloud Service Discovery</div> <div>Cloud Storage Object Discovery</div> <div>Container and Resource Discovery</div> <div>Debugger Evasion</div> <div>Device Driver Discovery</div> <div>Domain Trust Discovery</div> <div>File and Directory Discovery</div> <div>Group Policy Discovery</div> <div>Log Enumeration</div> <div>Network Service Discovery</div> <div>Network Share Discovery</div> <div>Network Sniffing</div> <div>Password Policy Discovery</div> <div>Peripheral Device Discovery</div> <div>Permission Groups Discovery (3)</div> <div>Process Discovery</div> <div>Query Registry</div> <div>Remote System Discovery</div> <div>Software Discovery (1)</div> <div>System Information Discovery</div> <div>System Location Discovery (1)</div> <div>System Network Configuration Discovery (2)</div> <div>System Network Connections Discovery</div> <div>System Owner/User Discovery</div> <div>System Service Discovery</div> <div>System Time Discovery</div> <div>Virtualization/Sandbox Evasion (3)</div> </div>	<div> <div>Exploitation of Remote Services</div> <div>Internal Spearphishing</div> <div>Lateral Tool Transfer</div> <div>Remote Service Session Hijacking (2)</div> <div>Remote Services (8)</div> <div>Replication Through Removable Media</div> <div>Software Deployment Tools</div> <div>Taint Shared Content</div> <div>Use Alternate Authentication Material (4)</div> </div>	<div> <div>Adversary-in-the-Middle (4)</div> <div>Archive Collected Data (3)</div> <div>Audio Capture</div> <div>Automated Collection</div> <div>Browser Session Hijacking</div> <div>Clipboard Data</div> <div>Data from Cloud Storage</div> <div>Data from Configuration Repository (2)</div> <div>Data from Information Repositories (5)</div> <div>Data from Local System</div> <div>Data from Network Shared Drive</div> <div>Data from Removable Media</div> <div>Data Staged (2)</div> <div>Email Collection (3)</div> <div>Input Capture (4)</div> <div>Screen Capture</div> <div>Video Capture</div> </div>	<div> <div>Application Layer Protocol (5)</div> <div>Communication Through Removable Media</div> <div>Content Injection</div> <div>Data Encoding (2)</div> <div>Data Obfuscation (3)</div> <div>Dynamic Resolution (3)</div> <div>Encrypted Channel (2)</div> <div>Fallback Channels</div> <div>Hide Infrastructure</div> <div>Ingress Tool Transfer</div> <div>Multi-Stage Channels</div> <div>Non-Application Layer Protocol</div> <div>Non-Standard Port</div> <div>Protocol Tunneling</div> <div>Proxy (4)</div> <div>Remote Access Software</div> <div>Traffic Signaling (2)</div> <div>Web Service (3)</div> </div>	<div> <div>Automated Exfiltration (1)</div> <div>Data Transfer Size Limits</div> <div>Exfiltration Over Alternative Protocol (3)</div> <div>Exfiltration Over C2 Channel</div> <div>Exfiltration Over Other Network Medium (1)</div> <div>Exfiltration Over Physical Medium (1)</div> <div>Exfiltration Over Web Service (4)</div> <div>Scheduled Transfer</div> <div>Transfer Data to Cloud Account</div> </div>	<div> <div>Account Access Removal</div> <div>Data Destruction (1)</div> <div>Data Encrypted for Impact</div> <div>Data Manipulation (3)</div> <div>Defacement (2)</div> <div>Disk Wipe (2)</div> <div>Endpoint Denial of Service (4)</div> <div>Financial Theft</div> <div>Firmware Corruption</div> <div>Inhibit System Recovery</div> <div>Network Denial of Service (2)</div> <div>Resource Hijacking (4)</div> <div>Service Stop</div> <div>System Shutdown/Reboot</div> </div>

THREAT ACTORS
HAVE OPTIONS ;)

Threat Actor Disruption Through Research

			Privilege Escalation 14 techniques	Defense Evasion 44 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Resource Development 8 techniques	Initial Access 10 techniques		Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Acquire Access	Content Injection		Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Acquire Infrastructure (8)	Drive-by Compromise		Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Manipulation (3)
Compromise Accounts (3)	Exploit Public-Facing Application		Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Defacement (2)
Compromise Infrastructure (8)	External Remote Services		Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Develop Capabilities (4)	Hardware Additions		Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Establish Accounts (3)	Phishing (4)		Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Financial Theft
Obtain Capabilities (7)	Replication Through Removable Media		Escape to Host	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Firmware Corruption
Stage Capabilities (6)	Supply Chain Compromise (3)		Event Triggered Execution (17)	Execution Guardrails (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (5)	Hide Infrastructure	Transfer Data to Cloud Account	Inhibit System Recovery
	Trusted Relationship		Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer		Network Denial of Service (2)
			Hijack Execution Flow (13)	File and Directory Permissions Modification (2)	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Resource Hijacking (4)
			Process Injection (12)	Hide Artifacts (12)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Service Stop
			Scheduled Task/Job (5)	Hijack Execution Flow (13)	Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Non-Standard Port		System Shutdown/Reboot
			Valid Accounts (4)	Impair Defenses (11)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (3)	Protocol Tunneling		
				Indicator Removal (10)	Steal Web Session Cookie	Network Service Discovery		Input Capture (4)	Remote Access Software		
				Masquerading (10)	Unsecured Credentials (8)	Network Share Discovery		Screen Capture	Traffic Signaling (2)		
				Modify Authentication Process (9)		Network Sniffing		Video Capture	Web Service (3)		
				Modify Cloud Compute Infrastructure (5)		Password Policy Discovery					
				Indirect Command Execution		Peripheral Device Discovery					
				Masquerading (10)		Permission Groups Discovery (3)					
				Modify System Image (2)		Process Discovery					
				Network Boundary Bridging (1)		Query Registry					
				Obfuscated Files or Information (14)		Remote System Discovery					
				Plist File Modification		Software Discovery (1)					
				Pre-OS Boot (5)		System Information Discovery					
						System Location Discovery (1)					
						System Network Configuration Discovery (2)					
						System Network Connections Discovery					
						System Owner/User Discovery					
						System Service Discovery					

Proactive defence
based on Pre-
ATT&CK
infrastructure
discovery

Threat Actor Disruption Through Research

The diagram illustrates the MITRE ATT&CK framework, organized into five main stages: Resource Development, Initial Access, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Command and Control, Exfiltration, and Impact. Each stage contains specific techniques, with some techniques being part of multiple stages.

Resource Development (8 techniques):

- Acquire Access
- Acquire Infrastructure (8)
- Compromise Accounts (3)
- Compromise Infrastructure (8)
- Develop Capabilities (4)
- Establish Accounts (3)
- Obtain Capabilities (7)
- Stage Capabilities (5)

Initial Access (10 techniques):

- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (4)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Privilege Escalation (14 techniques):

- Abuse Elevation Control Mechanism (6)
- Access Token Manipulation (5)
- Account Manipulation (7)
- Boot or Logon Autostart Execution (14)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (5)
- Domain or Tenant Policy Modification (2)
- Escape to Host
- Event Triggered Execution (17)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (13)
- Process Injection (12)
- Scheduled Task/Job (5)
- Valid Accounts (4)

Defense Evasion (44 techniques):

- Abuse Elevation Control Mechanism (6)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain or Tenant Policy Modification (2)
- Execution Guardrails (2)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (12)
- Hijack Execution Flow (13)
- Impair Defenses (11)
- Impersonation
- Indicator Removal (10)
- Indirect Command Execution
- Masquerading (10)
- Modify Authentication Process (9)
- Modify Cloud Compute Infrastructure (5)
- Modify Cloud Resource Hierarchy
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information (14)
- Plist File Modification
- Pre-OS Boot (5)

Credential Access (17 techniques):

- Adversary-in-the-Middle (4)
- Brute Force (4)
- Credentials from Password Stores (6)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (9)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Generation
- Network
- OS Credential Dumping
- Steal App Access Tokens
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (5)
- Steal Web Session Cookie
- Unsecured Credentials (8)

Discovery (32 techniques):

- Account Discovery (4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Location Discovery (1)
- System Network Configuration Discovery (2)
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery

Lateral Movement (9 techniques):

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (8)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Command and Control (18 techniques):

- Application Layer Protocol (5)
- Communication Through Removable Media
- Content Injection
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Hide Infrastructure
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software

Exfiltration (9 techniques):

- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (4)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact (4 techniques):

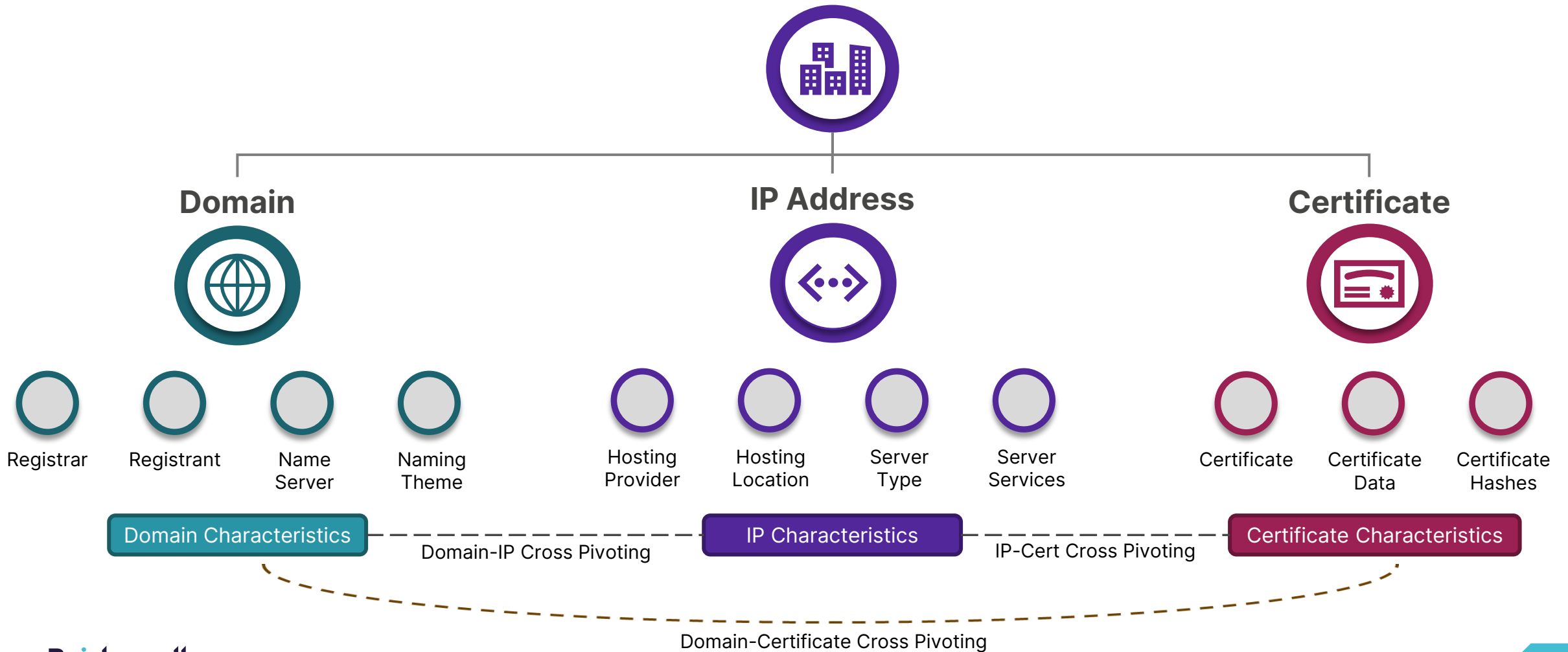
- Access Removal
- Destruction (1)
- Encryption for Manipulation (3)
- Cement (2)
- Wipe (2)
- Joint Denial of Service (4)
- Al Theft
- Corruption
- System Recovery
- Work Denial of Service (2)
- Source Hijacking (4)
- Stop
- Shutdown/Reboot

Proactive defence based on Pre-ATT&CK infrastructure discovery

Disrupt persistent attacks at the command-and-control and exfiltration stages

Malicious Infrastructure Pivots

Malicious Network Infrastructure



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



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](#) [List](#)

Product Spotlight: We've Launched a new

45.154.98.68

45.154.98.68.powered.by.rd
p.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"

TOTAL RESULTS

49

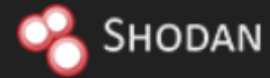
TOP COUNTRIES



Netherlands	18
United States	11
Poland	5
Germany	4
France	3
More...	

TOP PORTS

4444	12
444	9



ssl:"AsyncRAT Server"



Product Spotlight: We've Launched a new

45.154.98.68

45.154.98.68.powered.by.rd
p.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.



Cybercrime – Offensive Security Tools (OST)



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

Hunt Rules:

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

ssl:"multiplayer" ssl:"operators"

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:

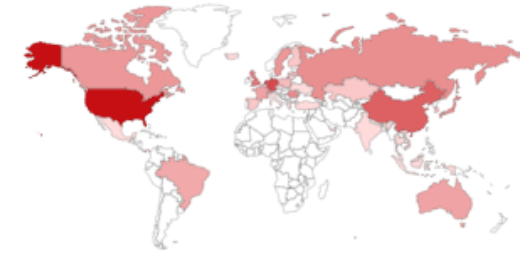
multiplayer

SSL Error: TLSV1_ALERT_PROTOCOL_VERSION

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.

The screenshot displays the GitHub interface for the `rapid7 / metasploit-framework` repository. The repository is public and has 423 issues, 39 pull requests, and 2054 watchers. The file explorer shows the `lib/msf/core/web_services/public/` directory, with `favicon.ico` highlighted. A search bar in the top right of the file explorer shows the search term `.ico`. The commit history on the right shows 76,351 commits, with the most recent commit made 1 hour ago.

rapid7 / metasploit-framework

Search: Type / to search

Code Issues 423 Pull requests 39 Discussions Actions Projects 1 Wiki Security

metasploit-framework Public Watch 2054

master 23 Branches 935 Tags

Search: .ico

lib/msf/core/web_services/public/favicon.ico Go to file

.github/ISSUE_TEMPLATE/config.yml

docs/metasploit-framework.wiki/The-ins-and-outs-of-HTTP-and-HTTPS-communications-in-Meterpreter-and-Metasploit-Stagers.md

.github/workflows/command_shell_acceptance.yml

docs/metasploit-framework.wiki/Contact.md

docs/metasploit-framework.wiki/Committer-Keys.md

8 · 1 hour ago 76,351 Commits

2 weeks ago

2 years ago

2 years ago

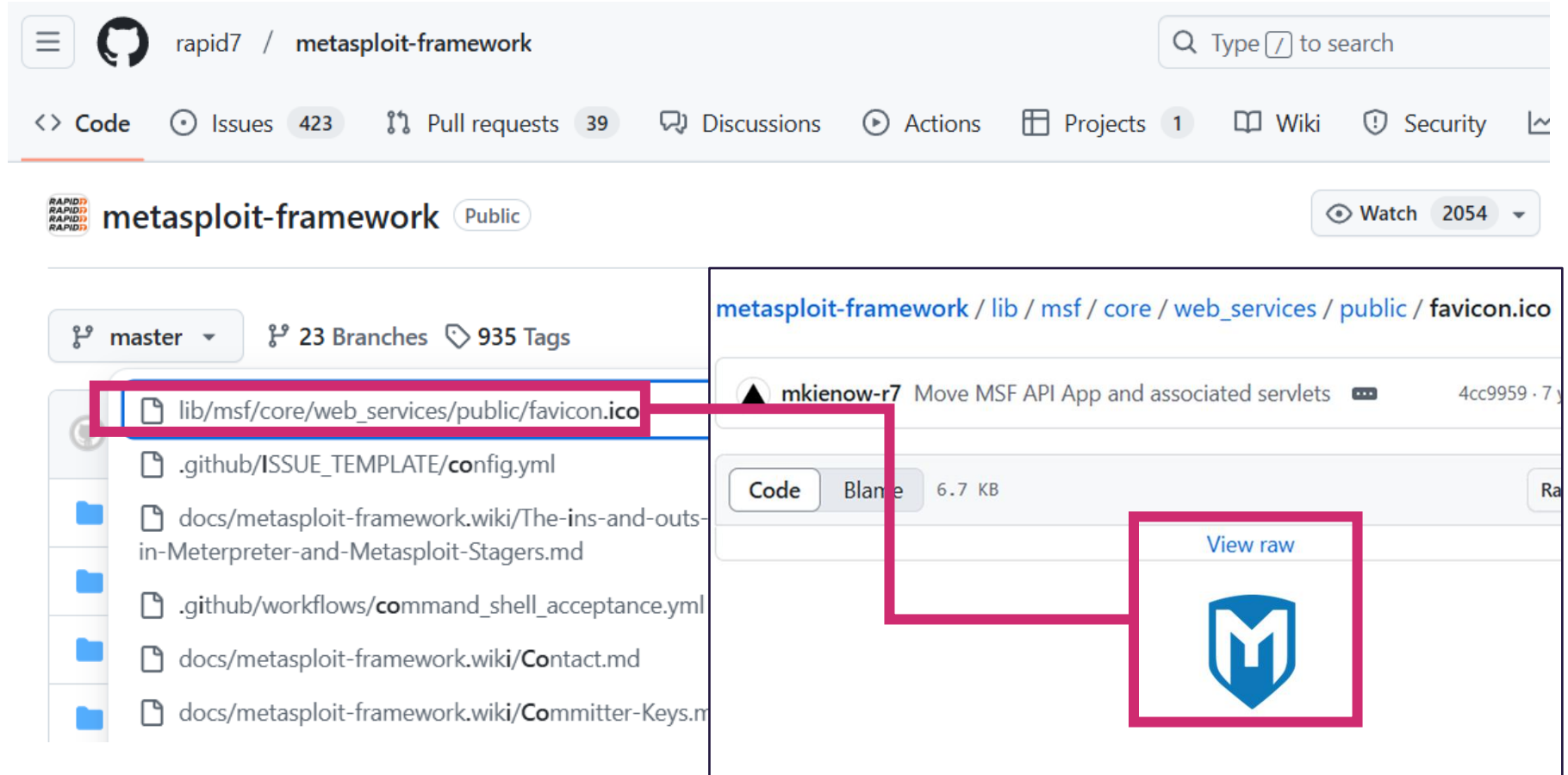
2 weeks ago

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"

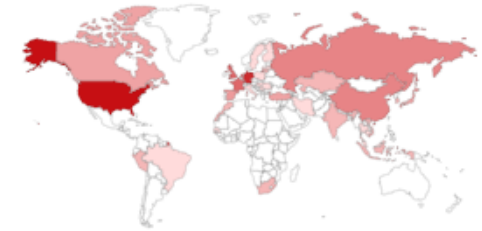
Favicon icon:

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

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...

2025-09-04T06:21:14.080768

8.148.194.157

Aliyun Computing Co.LTD

China, Guangzhou

cloud self-signed

SSL Certificate

Issued By:

| Common Name:

jquery.com

| Organization:

jQuery

Issued To:

| Common Name:

jquery.com

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

2025-09-04T05:48:34.447978

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.

23.94.59.4 

23-94-59-4-host.colocrossing.com
drive-microsoft.top
www.drive-microsoft.top
RackNerd LLC
United



```

⊕ cert: { ... },
⊕ chain: [ /* 1 item */ ],
⊕ chain_sha256: [ /* 1 item */ ],
⊕ cipher: { ... },
⊕ dhparams: { ... },
⊕ handshake_states: [ /* 12 items */ ],
ja3s: "fef5599f0a3662839aeb1f3c854eba06",
jarm: "07d14d16d21d21d00042d41d00041d47e4e0ae17960b2a5b4fd6107fbb0926",

```

SSL Certificate

Issued By:

|- Organization:
CloudFlare, Inc.

Issued To:

|- Common Name:
CloudFlare Origin
Certificate

|- Organization:
CloudFlare, Inc.

Supported SSL

Versions:

TLsv1.2, TLsv1.3

Diffie-Hellman

Fingerprint:

**RFC2409/Oakley
Group 2**

HTTP/1.1 404 Not Found

Date: Wed, 19 Feb 2025 19:05:00 GMT

Content-Type: text/plain

Content-Length: 0

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.

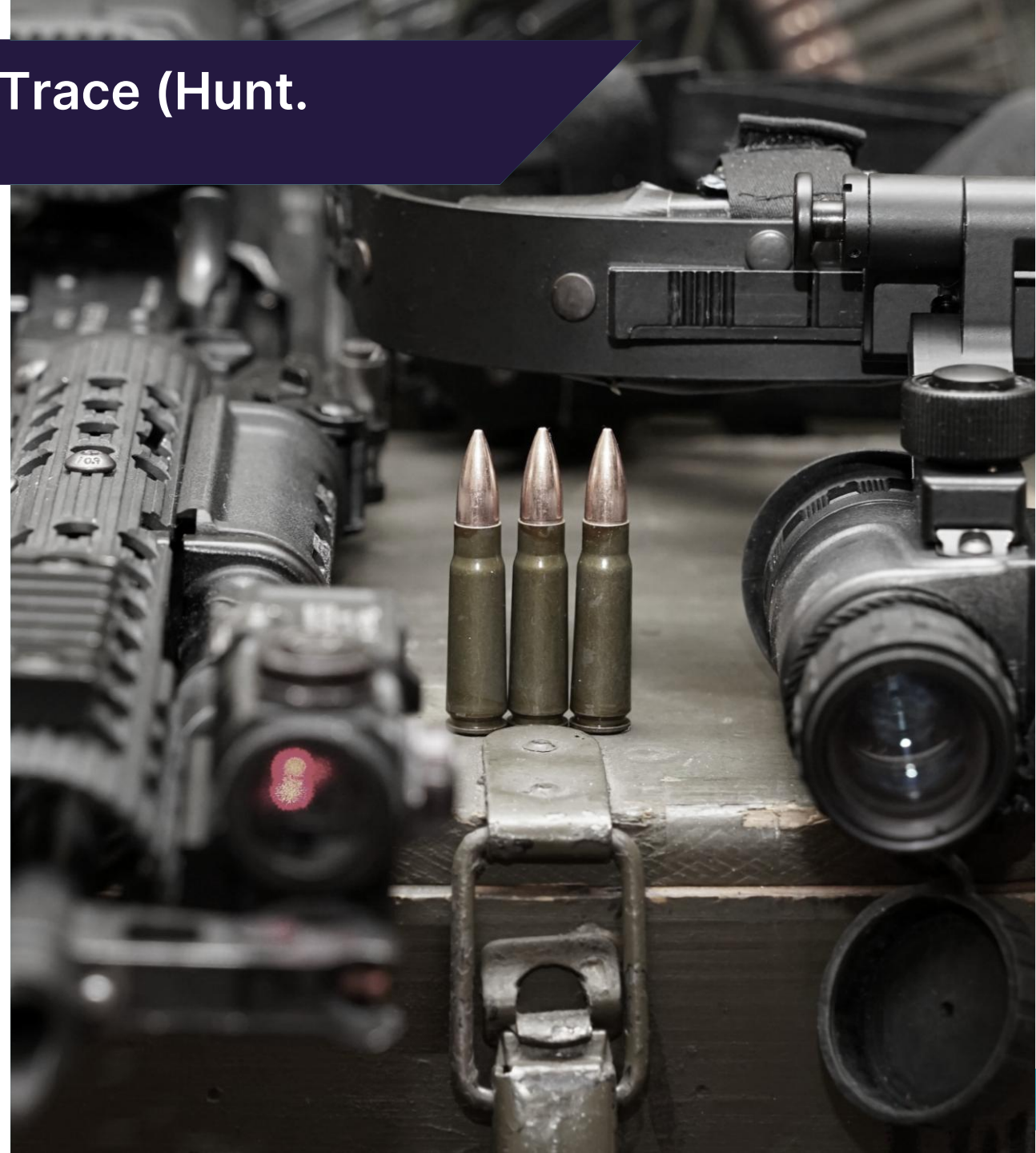
Your Tools:

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 !!!



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

