Cyber Threat Brief

CPT Sean McQuade (Regional Cyber Center – Pacific)

The Overall Classification for this Brief is UNCLASSIFIED

Disclaimer

The views and opinions presented herein are those of the author and do not necessarily represent the views of DoD or the Army. Appearance of, or reference to, any commercial products or services does not constitute DoD or Army endorsement of those products or services. The appearance of external hyperlinks does not constitute DoD or Army endorsement of the linked websites, or the information, products or services therein.

Agenda

- Cyber Threats in the News
- Defining Cyber Threat Intelligence (CTI)
- CTI Terminology
- CTI Technical Analysis
- MITRE ATT@CK – Enterprise
- Search Engine Optimization (SEO) Poisoning – Technique Overview
- Threat Actors
- Volt Typhoon – Campaign Overview
- Applying Army Doctrine to Cyberspace to Mitigate Organizational Risk
- Closing Remarks

Cyber Threats in the News

WSJ

FBI Director Says China Cyberattacks on U.S. Infrastructure Now at Unprecedented Scale

Christopher Wray warns that pre-positioned malware could be triggered to disrupt critical systems in the U.S..

BBC

North Korea hacked emails of South Korea president's aide

North Korea hacked into the personal emails of an aide to the South Korean president, his office has confirmed to the BBC. The breach occurred in the run-up...

Reuters

Microsoft says it caught hackers from China, Russia and Iran using its AI tools

State-backed hackers from Russia, China, and Iran have been using tools from Microsoft-backed OpenAI to hone their skills and trick their...

Defining Cyber Threat Intelligence (CTI)

Analyzed information about the hostile intent, opportunity, and capability of an adversary that satisfies a requirement. SANS

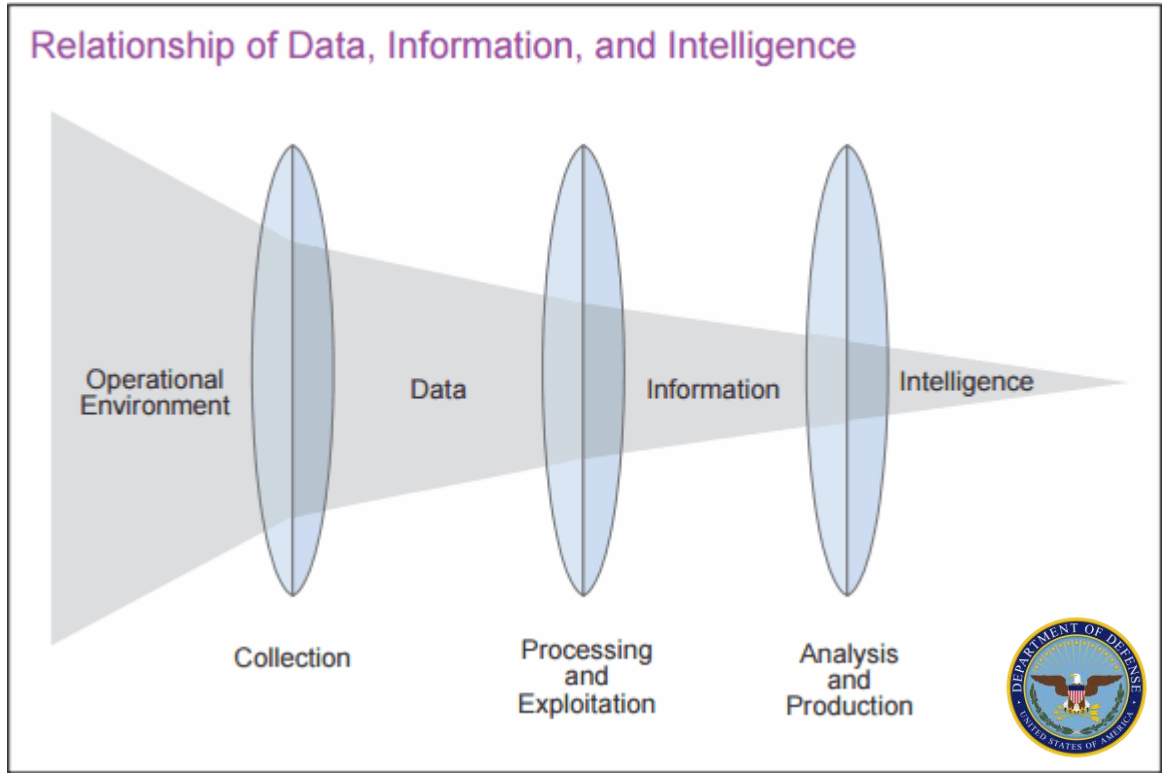
Threat + Vulnerability + Impact

Adversary Capability & Intent

System Weaknesses

Operational Impairment to a CDR's Mission

= Risk



CTI Terminology

Adversary / Threat Actor	Intelligence Requirement	Indicator	Common Vulnerabilities and Exposure (CVE)
Intrusion	Activity Group	Campaign	Target vs. Victim
Persona	Advanced Persistent Threat	Tactic, Technique, Procedure (TTP)	Tradecraft

SANS

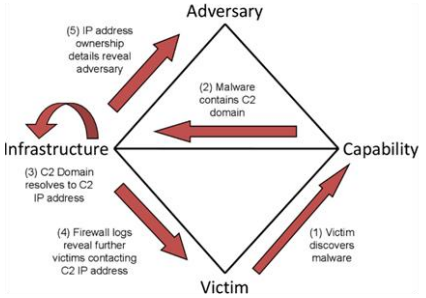
Alerts and Advisories – CISA

CTI Technical Analysis

We use structured analytic techniques to analyze activity on the DoDIN to provide meaningful information to support leadership decisions, defenders' needs, and Intelligence efforts.

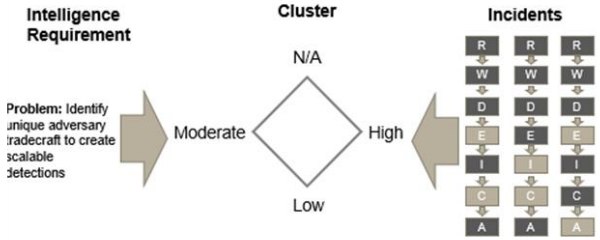
KILL CHAIN

DIAMOND MODEL



ATT&CK FRAMEWORK

CTI Analysis



MITRE ATT@CK – Enterprise

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	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
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	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	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	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)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	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)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Domain 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)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Escape to Host	Direct Volume Access	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Ingress Tool Transfer	Transfer Data to Cloud	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Multi-Stage Channels		Inhibit System Recovery
			Software Deployment Tools			Exploitation for Defense Evasion		Domain Trust Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service (2)
			System Services (2)			File and Directory Permissions Modification (2)		File and Directory Discovery			Non-Standard Port		Resource Hijacking
						Hide Artifacts (11)		Group Policy Discovery					Service Stop
								Log Enumeration					

MITRE ATT&CK

Search Engine Optimization (SEO) Poisoning – Technique Overview

UNCLASSIFIED

SEO Poisoning

- A technique used by threat actors to increase the prominence of their malicious websites. SEO poisoning tricks the human mind by users assuming the top hits are the most credible and is effective when people fail to look closely at their search results.

- Threat actors may employ targeted types of SEO poisoning, like spearphishing, to go after specific users, like IT administrators. This customization enables attackers to target and customize their attacks to specific audiences, making them more challenging to identify and defend against.

CROWDSTRIKE

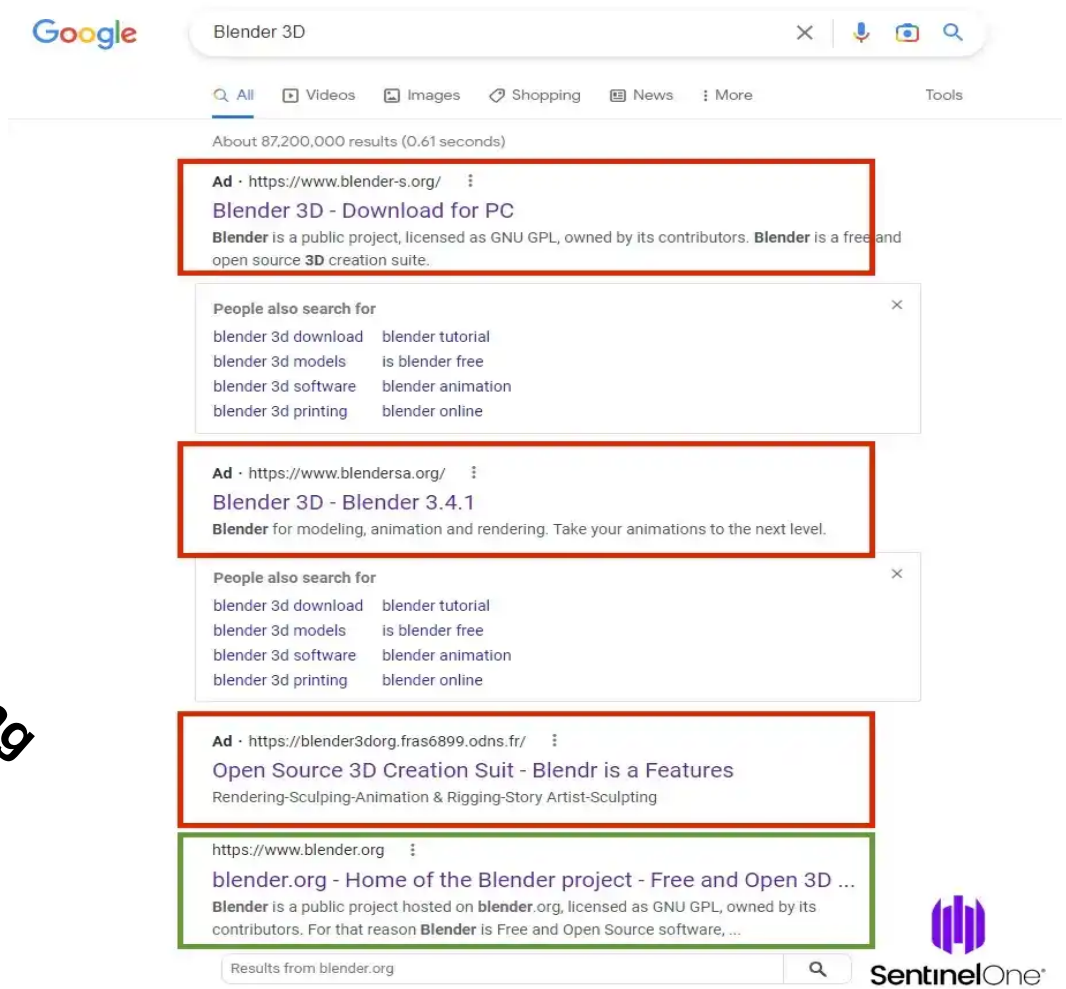
SEO Poisoning

Legitimate Website: blender.org

The three malicious ads link to:

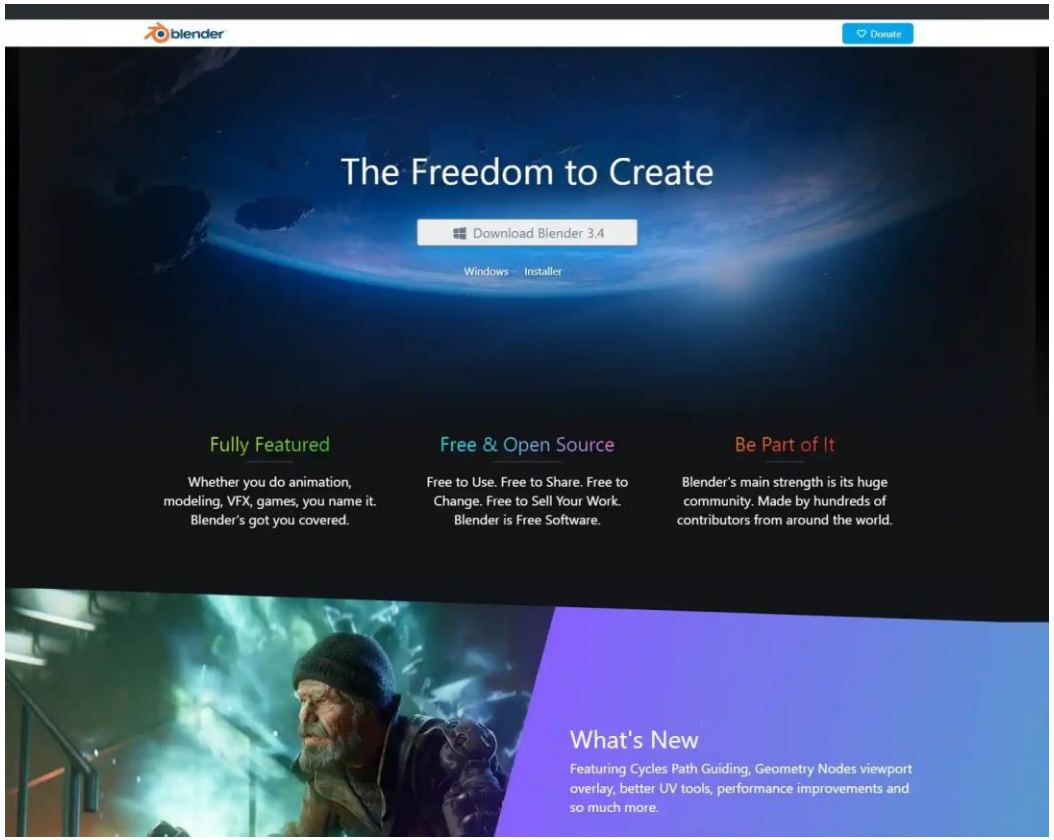
- blender-s.org
- blendersa.org
- blender3dorg.fras6899.odns.fr

Typosquatting

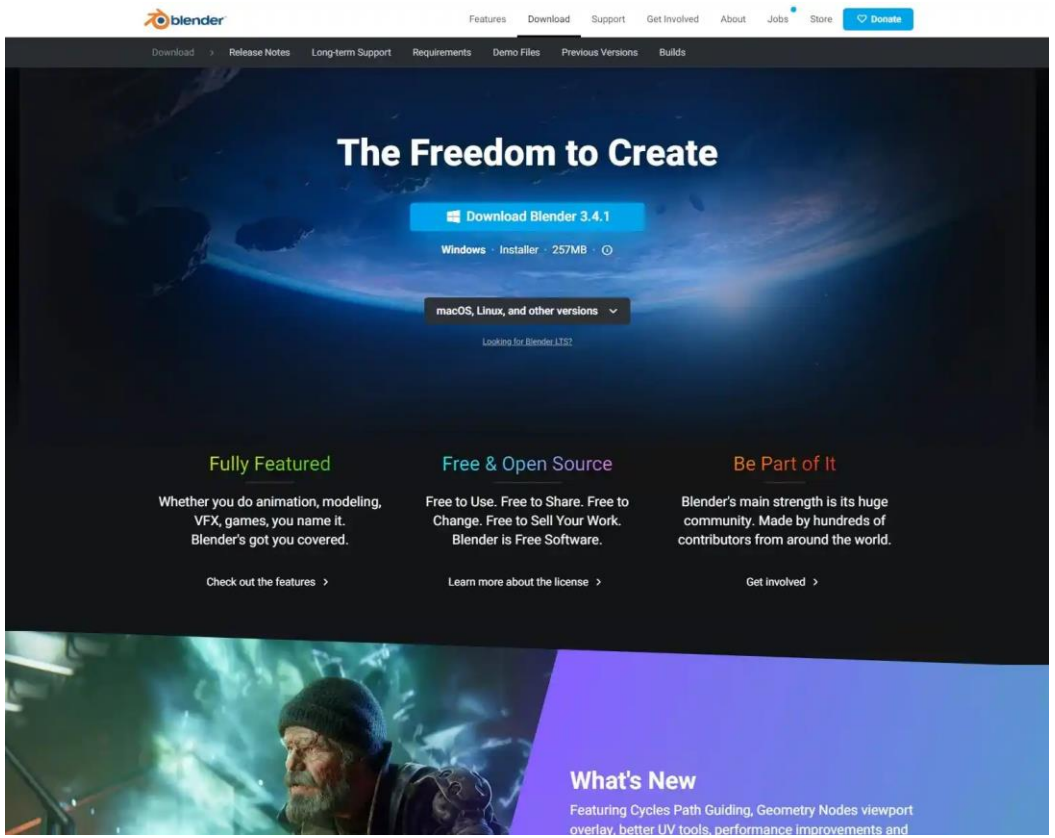


SentinelOne

SEO Poisoning



Malicious Website



Legitimate Website

MITRE ATT@CK – Enterprise

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	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
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	BITS Jobs	Account Manipulation (6)	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Build Image on Host	Boot or Logon Autostart Execution (14)	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Debugger Evasion	Boot or Logon Initialization Scripts (5)	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Deploy Container	Create or Modify System Process (4)	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Direct Volume Access	Domain Policy Modification (2)	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Domain Policy Modification (2)	Execution Guardrails (1)	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Escape to Host	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Ingress Tool Transfer	Transfer Data to Cloud	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Event Triggered Execution (16)	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Multi-Stage Channels		Inhibit System Recovery
			Software Deployment Tools		Exploitation for Privilege Escalation	Hide Artifacts (11)		Domain Trust Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service (2)
			System Services (2)					File and Directory Discovery			Non-Standard Port		Resource Hijacking
								Group Policy Discovery					Service Stop
								Log Enumeration					

MITRE ATT&CK

SEO Poisoning

Resource Development – Acquire Infrastructure – Malvertising Sub-Technique (T1583.008)

- Adversaries may purchase online advertisements that can be abused to distribute malware to victims.
- Ads can be purchased to plant as well as favorably position artifacts in specific locations online, such as prominently placed within search engine results.
- Purchased ads may also target specific audiences using the advertising network's capabilities, potentially further taking advantage of the trust inherently given to search engines and popular websites.

SEO Poisoning

Initial Access – Drive-by Compromise Technique (T1189)

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation.

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack.

MITRE ATT&CK

SEO Poisoning

Initial Access – Drive-by Compromise Technique (T1189)

Multiple ways of delivering exploit code to a browser exist including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting
- Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary
- Malicious ads are paid for and served through legitimate ad providers (i.e., Malvertising)
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client.

MITRE ATT&CK

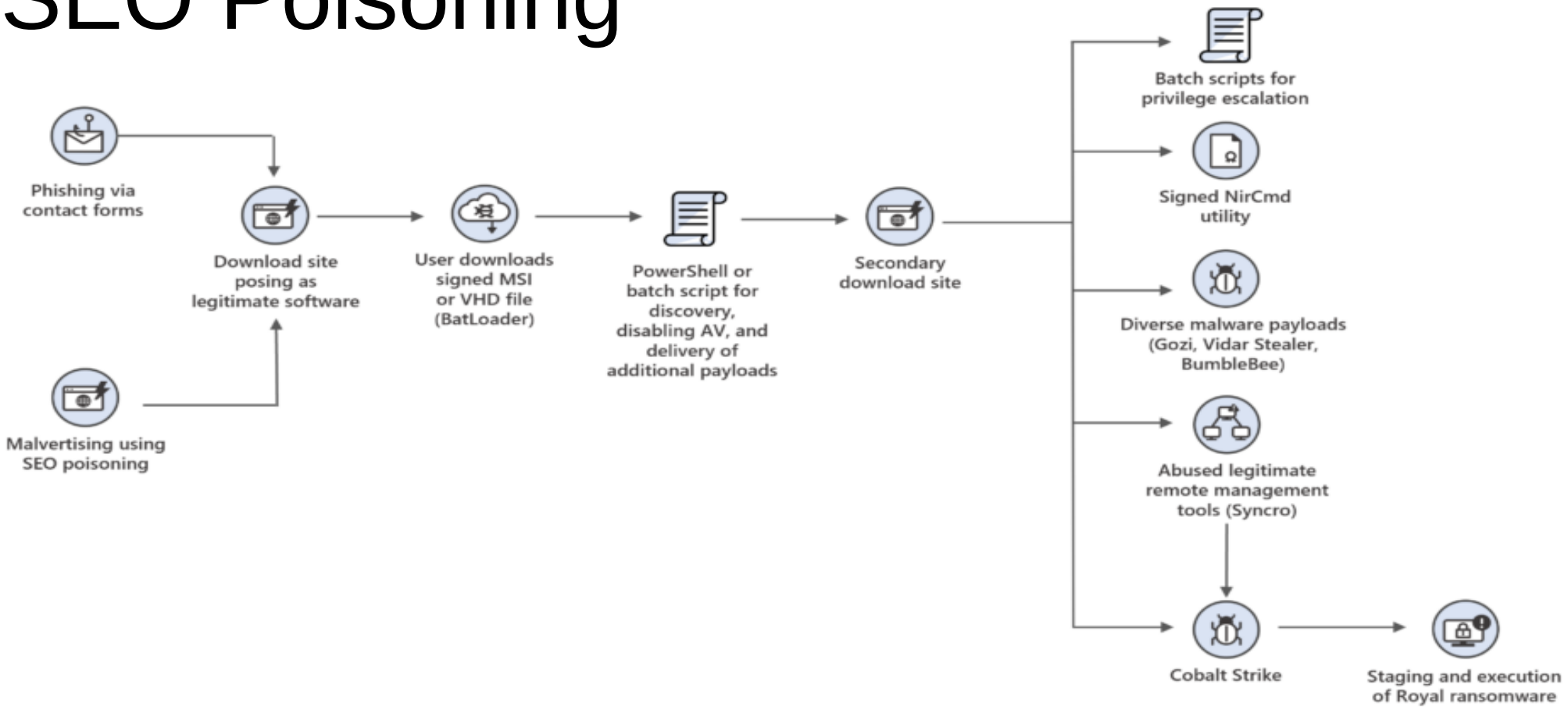
SEO Poisoning

Initial Access – Drive-by Compromise Technique (T1189)

Typical drive-by compromise process:

- A user visits a website that is used to host the adversary-controlled content.
- Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version.
- Upon finding a vulnerable version, exploit code is delivered to the browser.
- If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place.

SEO Poisoning



Microsoft

Threat Actors

- Nation States
- Criminal Organizations
- Hacktivists
- Insider Threats

UNCLASSIFIED

Threat Actors – Trends

Most impactful threat actor

LockBit

Category	Cybercriminal
Motive	Financial gain
Likelihood	Probable
Impact	High

LockBit is agile, evading law enforcement and targeting all industries globally. LockBit operates a very successful Ransomware-as-a-service (RaaS) model. [3]

Most trending threat actor

Volt Typhoon

Category	Nation-state affiliated
Motive	Corporate and political gain
Likelihood	Probable
Impact	Moderate

Volt Typhoon lifted the defense evasion bar with their living-off-the-land (LOTL) techniques. They perform stealthy cyber espionage campaigns across multiple industries. [107]

Top threat vector

Ransomware

Tactic	TA0040
Likelihood	Likely
Impact	Severe

Ransom demand reached up to $80 million in 2023, but in an encouraging trend, some businesses – in collaboration with law enforcement - are no longer paying the ransom. [2]

Top trend observed by operations

Dynamic Link Library (DLL) abuse

Tactic	TA0002, TA0004, TA0005
Likelihood	Likely
Impact	Moderate

Operations noted Dynamic Link Library (DLL) abuse through infected Universal Serial Bus (USB) drives, highlighting the persisting trend of threat actors re-using old methods and infrastructure. [1]

Deloitte.

Multiple Threat Actor Naming Conventions

Threat Group-3390 (MITRE)	APT 27 (Mandiant)	Emissary Panda (Crowdstrike)	Bronze Union (SecureWorks)
Earth Smilodon (Trend Micro)	Iron Tiger (Trend Micro)	LuckyMouse (Kaspersky)	Iron Taurus (Palo Alto)

Example: Threat Group-3390 is a Chinese threat group that has extensively used strategic web compromises to target victims. The group has been active since at least 2010 and has targeted organizations in the aerospace, government, defense, technology, energy, manufacturing and gambling/betting sectors.

MITRE ATT&CK

Microsoft Naming Convention

Blizzard
Russia

Sleet
North Korea

Typhoon
China

Sandstorm
Iran

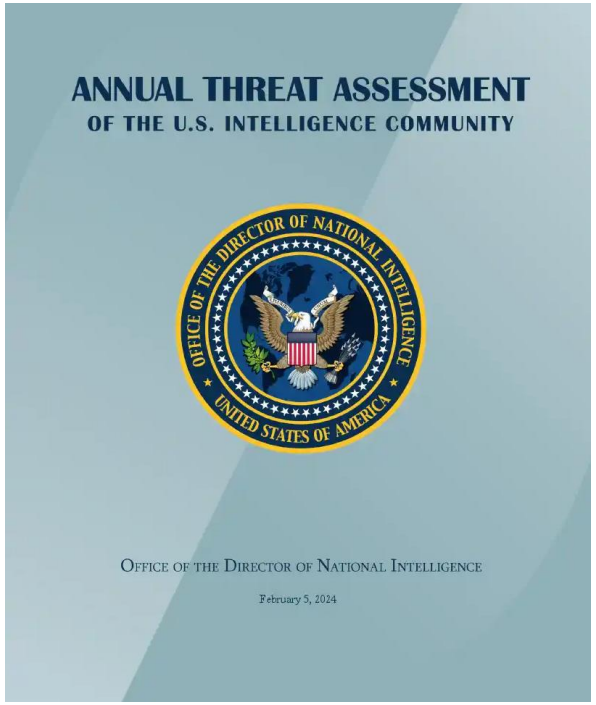
Storm
Groups in development

Tempest
Financially motivated

Tsunami
Private sector offensive actor

Flood
Influence operations

2024 Intelligence Estimate



The Russian Federation

***Russia (RF) will pose an enduring global Cyber threat even as it prioritizes cyber operations for the Ukrainian war*.** Moscow views Cyber disruptions as a foreign policy lever to shape other countries' decisions and continuously refines and employs its espionage, influence, and attack capabilities against a variety of targets.

• Russia maintains its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries.

APTs by Country - RF

Microsoft (Mandiant)

Aqua Blizzard (UNC530)	Cadet Blizzard	Forest Blizzard (APT 28)	Ghost Blizzard
Midnight Blizzard (APT 29)	Seashell Blizzard	Secret Blizzard	Star Blizzard
Storm-0587	Storm-1099	Sunglow Blizzard	

The Democratic People's Republic of Korea

North Korea's (DPRK) Cyber program will pose a sophisticated and agile espionage, Cybercrime, and attack threat. Pyongyang's Cyber forces have matured and are fully capable of achieving a variety of strategic objectives against diverse targets, including a wider target set in the United States and South Korea.

North Korea will continue its ongoing Cyber campaign, particularly cryptocurrency heists; seek a broad variety of approaches to launder and cash out stolen cryptocurrency; and maintain a program of IT workers serving abroad to earn additional funds.

APTs by Country - DPRK

Microsoft (Mandiant)

- Citrine Sleet (UNC4736)
- Diamond Sleet
- Emerald Sleet
- Jade Sleet
- Onyx Sleet
- Opal Sleet
- Pearl Sleet
- Ruby Sleet
- Sapphire Sleet
- Storm-0530

The People's Republic of China

China (PRC) remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks. Beijing's Cyber espionage pursuits and its industry's export of surveillance, information, and communications technologies increase the threats of aggressive Cyber operations against the United States and the suppression of the free flow of information in Cyberspace.

• PRC operations discovered by the U.S. private sector probably were intended to pre-position Cyber attacks against infrastructure in Guam and to enable disrupting communications between the United States and Asia.

• If Beijing believed that a major conflict with the United States were imminent, it would consider aggressive Cyber operations against U.S. critical infrastructure and military assets. Such a strike would be designed to deter U.S. military action by impeding U.S. decisionmaking, inducing societal panic, and interfering with the deployment of U.S. forces.

Microsoft (Mandiant)

APTs by Country - PRC

Brass Typhoon (APT 41)	Charcoal Typhoon	Circle Typhoon	Volt Typhoon
Flax Typhoon	Gingham Typhoon (APT 40)	Granite Typhoon	Lilac Typhoon
Mulberry Typhoon (APT 5)	Nylon Typhoon (APT 15)	Raspberry Typhoon (APT 30)	Salmon Typhoon (APT 4)
Silk Typhoon	Storm-0062	Storm-0558	Violet Typhoon

Volt Typhoon – Campaign Overview

Volt Typhoon – Campaign Overview

Volt Typhoon – Naming Conventions

Volt Typhoon (Microsoft)	G1017 (MITRE)	Bronze Silhouette (Secure Works)	Vanguard Panda (CrowdStrike)
DEV-0391 (Palo Alto)	Insidious Taurus (Palo Alto)	Voltzite (Dragos)	UNC3236 (Mandiant)

MITRE ATT&CK

Volt Typhoon – Timeline

Activity Timeline

Dragos has observed VOLTZITE since early 2023, but they are assessed with low confidence to have been active as far back as 2021, and have potential overlaps with KOSTOVITE, another Dragos-tracked threat group. The following provides a high-level timeline of VOLTZITE-related incidents tracked by Dragos.

2023

EARLY
- US Territory of Guam compromise.

JUN
- **VOLTZITE** infiltrates United States emergency management organization.

JUL
- Dragos discovers **VOLTZITE** targeting African electric transmission and distribution providers.

NOV
- Dragos collaborated with E-ISAC on analysis of **VOLTZITE** activity against multiple US-based electric sector organizations.

DEC
- Dragos discovered evidence that **VOLTZITE** has overlaps with UTA0178, a threat activity cluster tracked by Volexity, exploiting Ivanti ICS VPN zero-day vulnerabilities.

2024

JAN
- Extensive reconnaissance of a US telecommunication's providers external network gateways.
- Evidence of compromise against a large US city's emergency services GIS network.

DRAGOS

May 2023 – Microsoft Report

Microsoft Security | Solutions | Products | Services | Partners | Resources | Contact Sales | Start free trial | All Microsoft | Search | Light | Dark

Blog home / Threat intelligence

Search the blog

Research Threat intelligence Microsoft Defender Threat actors · 10 min read

Volt Typhoon targets US critical infrastructure with living-off-the-land techniques

By Microsoft Threat Intelligence

May 24, 2023

Microsoft Defender XDR

Living off the land

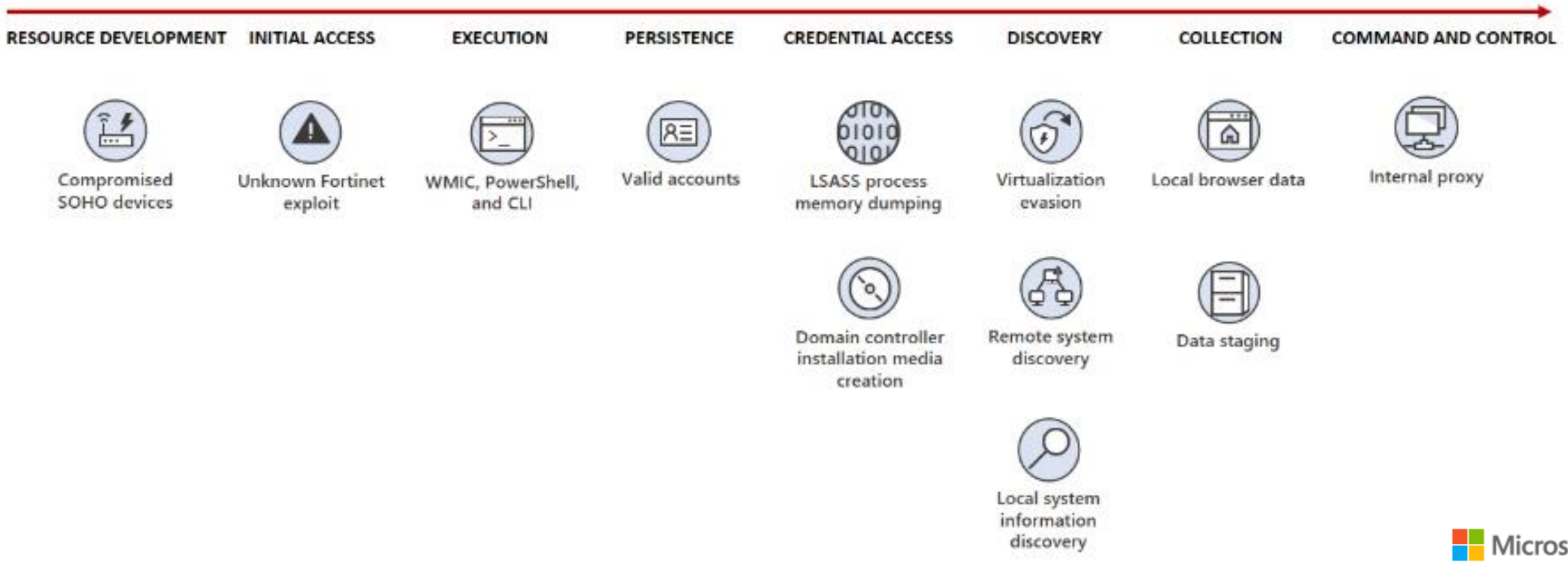
State-sponsored threat actor

more

Microsoft has uncovered stealthy and targeted malicious activity focused on post-compromise credential access and network system discovery aimed at critical infrastructure organizations in the United States. The attack is carried out by Volt Typhoon, a state-sponsored actor based in China that typically focuses on espionage and information gathering. Microsoft assesses with moderate confidence that this Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises.

Microsoft

Volt Typhoon – Attack Diagram



Microsoft

Credential Dumping

- Microsoft observed Volt Typhoon attempting to dump credentials through the Local Security Authority Subsystem Service (LSASS).
- The LSASS process memory space contains hashes for the current user's operating system (OS) credentials.

```
cmd.exe /c powershell -exec bypass -W hidden -nop -E
cgB1AG4AZABsAGwAMwAyAC4AZQB4AGUAIABDADoAXABXAGkAbgBkAG8AdwBzAFwAUwB5AHMAdABlA
G0AMwAyAFwAYwBvAG0AcwB2AGMAcwAuAGQAbABsACwAIABNAGkAbgBpAEQAdQBtAHAAIAA1ADUAMg
AgAEMAOgBcAFcAaQBuAGQAbwB3AHMAXABUAGUAbQBwAFwAdgBtAHcAYQByAGUALQB2AGgAbwBzAHQ
ALgBkAG0AcAAgAGYAdQBsAGwA
```

Command to dump LSASS process memory, encoded in Base64

```
rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump 552
C:\Windows\Temp\vmware-vhost.dmp full
```

Decoded Base64 of Volt Typhoon command to dump LSASS process memory

Microsoft

Create Installation Media

- Volt Typhoon frequently attempts to use the command-line tool Ntdsutil.exe to create installation media from domain controllers, either remotely or locally.

- The files in the installation media contain usernames and password hashes that actors can crack offline, giving them valid domain account credentials they could use to regain access to a compromised organization if they lose access.

```
wmic /node:[redacted] /user:[redacted]/password:
[redacted] process call create "cmd.exe /c mkdir C:\Windows\Temp\tmp
& ntdsutil \"ac i ntds\" ifm \"create full C:\Windows\Temp\tmp\" q q"
```

Command to remotely create domain controller installation media

```
cmd.exe /c  ntdsutil "ac i ntds" ifm "create full C:\Windows\Temp\pro" q q
```

Command to locally create domain controller installation media

Microsoft

May 2023 – Joint Cybersecurity Advisory

Joint Cybersecurity Advisory

TLP:CLEAR

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

Summary

The United States and international cybersecurity authorities are issuing this joint Cybersecurity Advisory (CSA) to highlight a recently discovered cluster of activity of interest associated with a People's Republic of China (PRC) state-sponsored cyber actor, also known as Volt Typhoon. Private sector partners have identified that this activity affects networks across U.S. critical infrastructure sectors, and the authoring agencies believe the actor could apply the same techniques against these and other sectors worldwide.

Joint Cybersecurity Advisory

Windows Management Instrumentation

- Volt Typhoon has executed the following command to gather information about local drives:

```
cmd.exe /C "wmic path win32_logicaldisk get
caption,filesystem,freespace,size,volumename"
```

- The command uses a command prompt WMIC query, collecting information about the storage devices on the local host. This command does not require administrative credentials to return results.

- WMI is a built-in Windows tool that allows a user to access management information from hosts in an enterprise environment. **By default, WMI Tracing is not enabled, so the WMI commands being executed and the associated user might not be available.**

Joint Cybersecurity Advisory

Port Proxy - Netsh

- Volt Typhoon has used the following commands to enable port forwarding on hosts:

```
"cmd.exe /c "netsh interface portproxy add v4tov4
listenaddress=0.0.0.0 listenport=9999
connectaddress=<rfc1918 internal ip address>
connectport=8443 protocol=tcp""
```

```
"cmd.exe /c netsh interface portproxy add v4tov4
listenport=50100 listenaddress=0.0.0.0 connectport=1433
connectaddress=<rfc1918 internal ip address>"
```

- Netsh is a built-in Windows command line scripting utility that can display or modify the network settings of a host, including the Windows Firewall. The portproxy add command is used to create a host:port proxy that will forward incoming connections.

- Netsh is a built-in Windows command line scripting utility that can display or modify the network settings of a host, including the Windows Firewall. **Using port proxies is not common for legitimate system administration since they can constitute a backdoor into the network that bypasses firewall policies.**

Joint Cybersecurity Advisory

February 2024 – Cybersecurity Advisory

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Menu

Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory

SHARE:

CYBERSECURITY ADVISORY

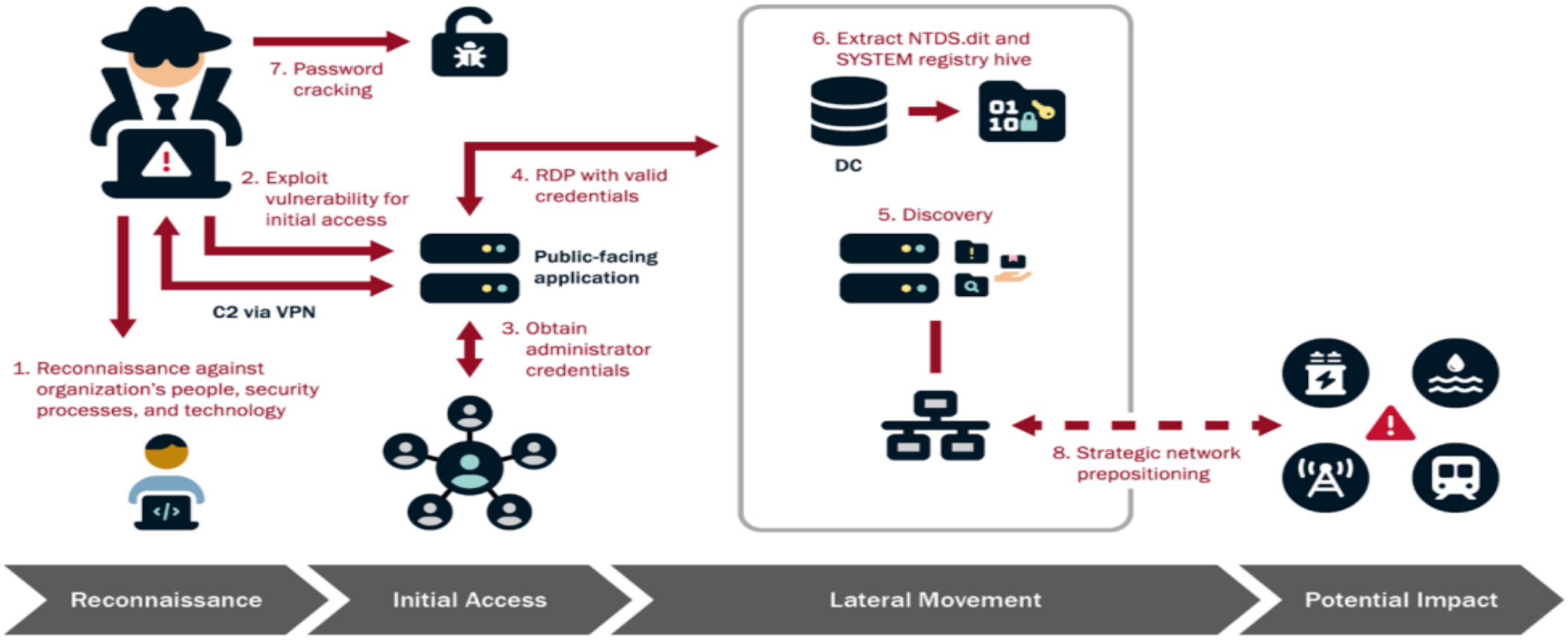
PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

Release Date: February 07, 2024

Alert Code: AA24-038A

RELATED TOPICS: NATION-STATE CYBER ACTORS, CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE, CYBER THREATS AND ADVISORIES

Volt Typhoon – Typical Activity



Volt Typhoon – Typical Activity

ACTIONS TO TAKE TODAY TO MITIGATE VOLT TYPHOON ACTIVITY:

1. Apply patches for internet-facing systems. Prioritize patching critical vulnerabilities in appliances known to be frequently exploited by Volt Typhoon.
2. Implement phishing-resistant MFA.
3. Ensure logging is turned on for application, access, and security logs and store logs in a central system.
4. Plan "end of life" for technology beyond manufacturer's supported lifecycle.

Applying Army Doctrine to Mitigate Organizational Risk

Traditional Battlefields

SUPPORT ZONE (SZ)

Designed to be free of significant enemy action and permit effective logistics and administration .

- Camouflage, Concealment, Cover, and Deception measures to protect from precision attack
- A sanctuary that is noncontiguous with other zones in the AOR

BATTLE ZONE (BZ)

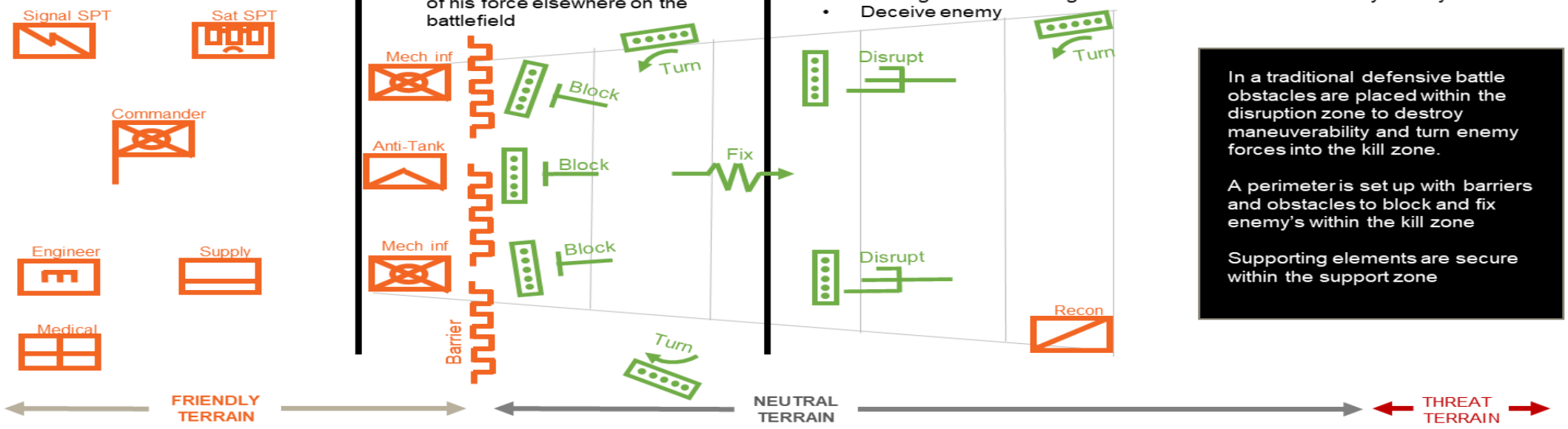
Conduct decisive actions to exploit opportunities created by actions in the disruption zone.

- Draw enemy attention and resources to action
- Hold terrain
- Inflict casualties on vulnerable enemy units
- Prevent enemy from moving a part of his force elsewhere on the battlefield

DISRUPTION ZONE (DZ)

Area in which the unit's disruption force will conduct disruption task to set conditions for successful combat actions by fixing enemy forces and placing fire on them.

- Attack enemy's engineer elements to destroy maneuverability in complex terrain.
- Strip away enemy's reconnaissance and deny him the ability to acquire and engage
- Disrupt offensive preparation
- Gaining and maintaining reconnaissance contact with key enemy elements
- Deceive enemy

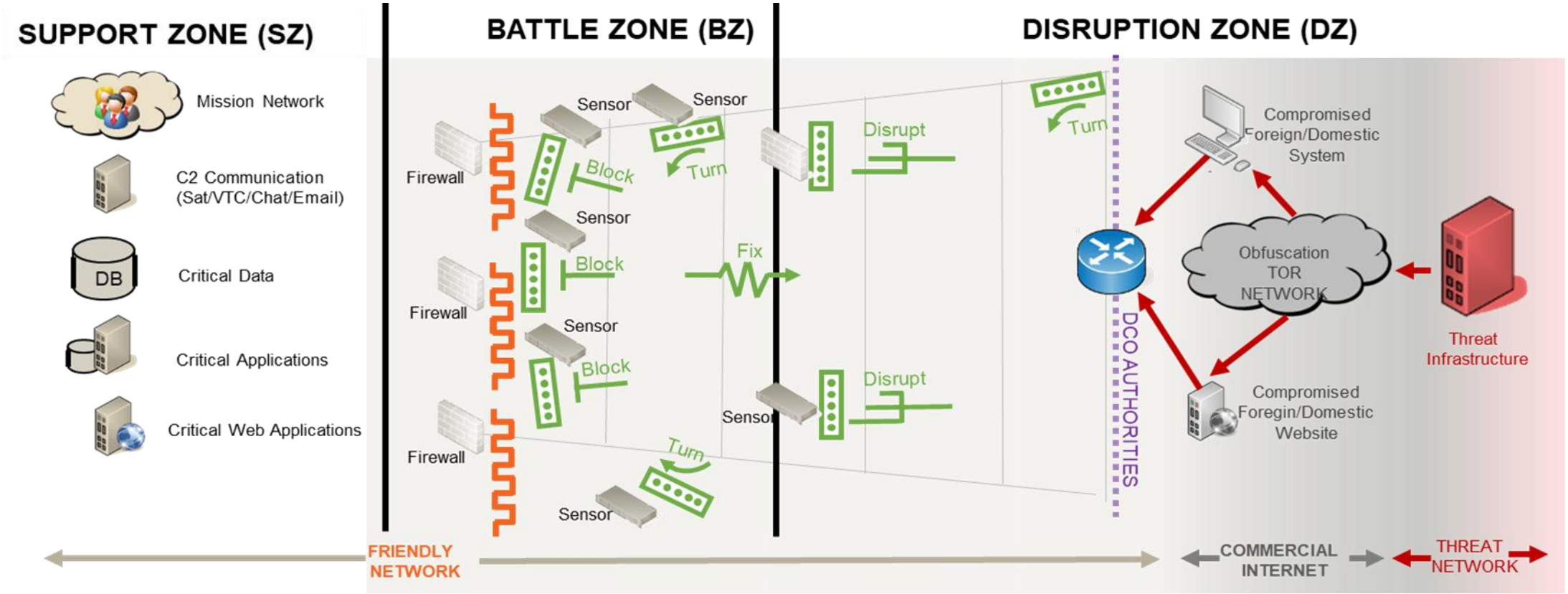


In a traditional defensive battle obstacles are placed within the disruption zone to destroy maneuverability and turn enemy forces into the kill zone.

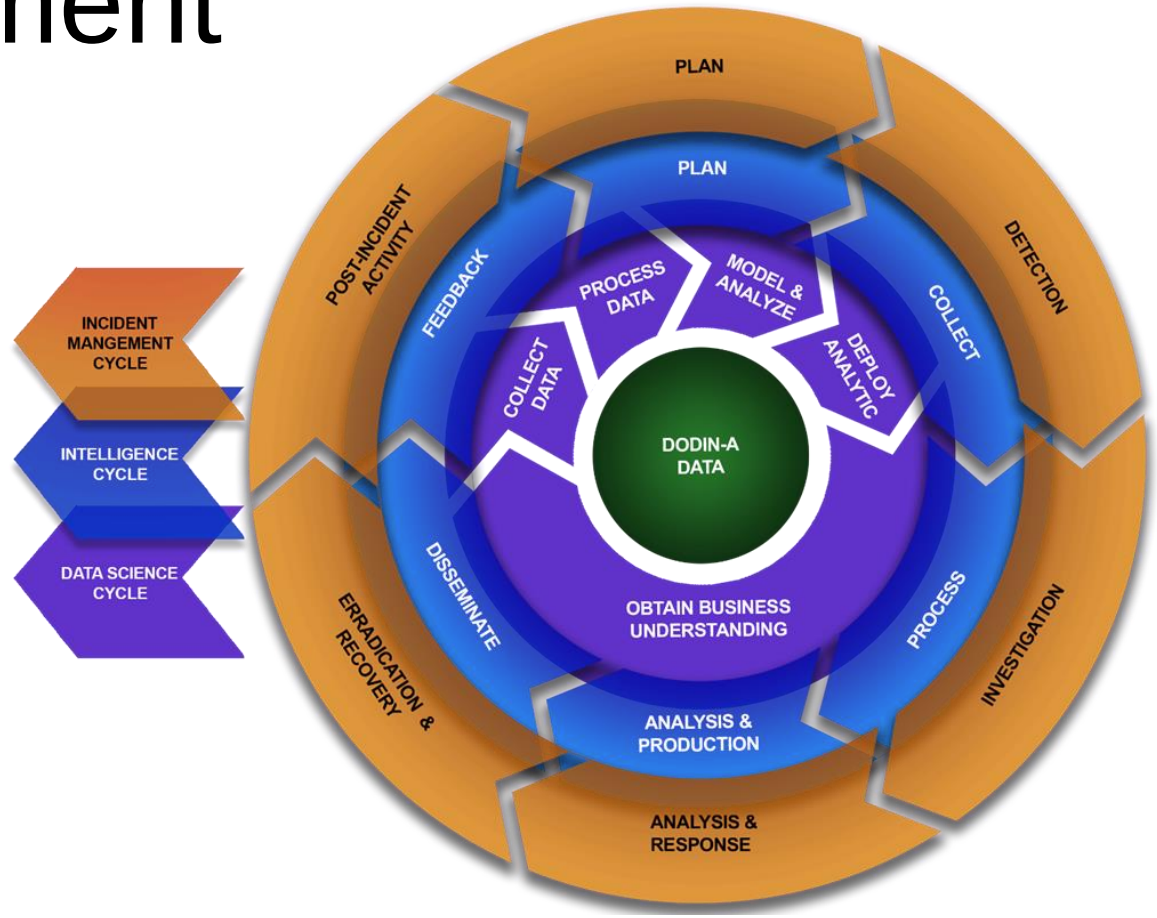
A perimeter is set up with barriers and obstacles to block and fix enemy's within the kill zone

Supporting elements are secure within the support zone

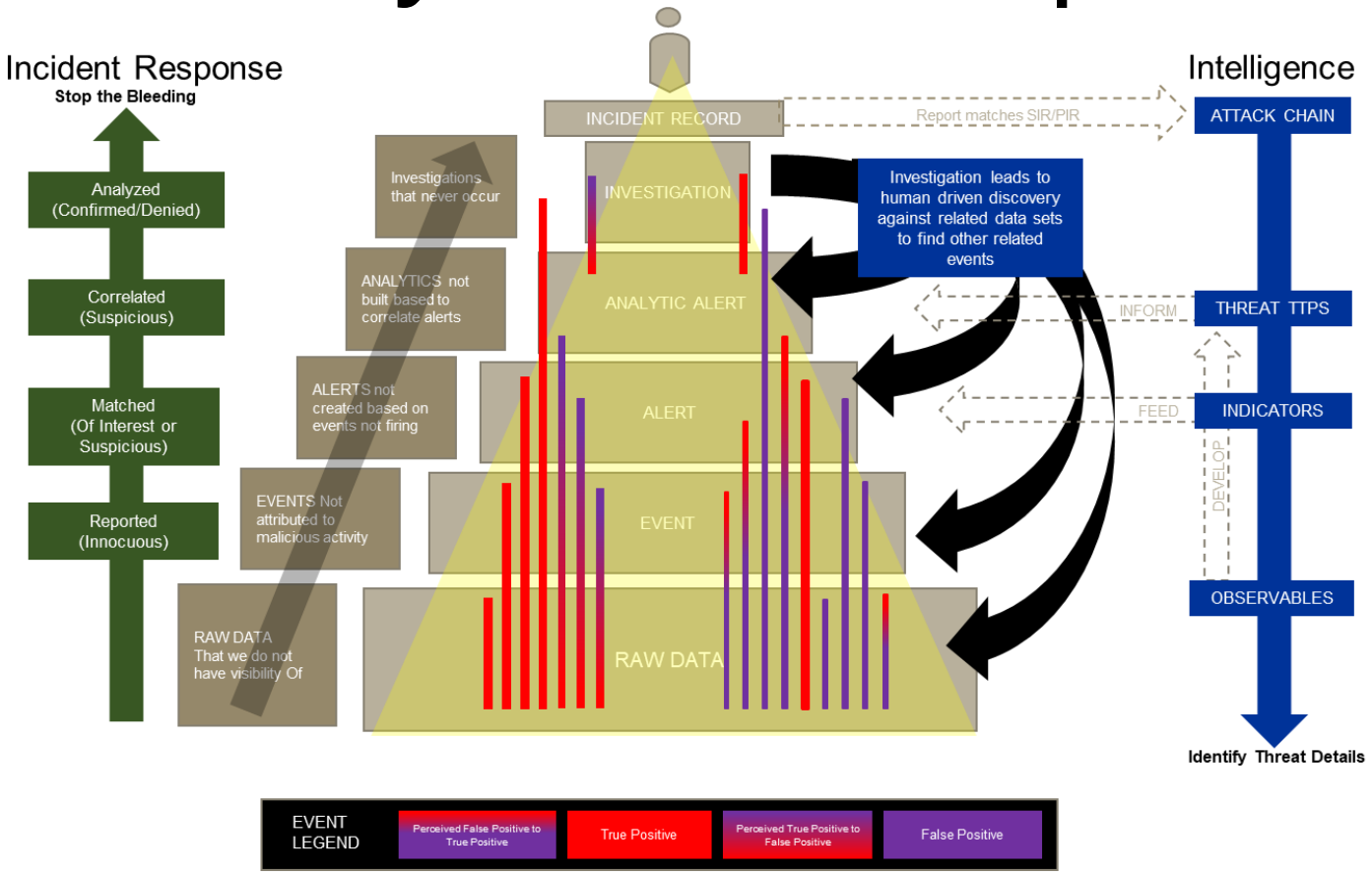
A Theoretical Battlefield in Cyberspace



Synchronizing Intelligence and Incident Management



How Do Intelligence Efforts Use Incident Data To Identify And Fill Gaps?



Closing Remarks

UNCLASSIFIED