CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

PEOPLE'S REPUBLIC OF CHINA THREAT

Charlie Marmon,
Cybersecurity Coordinator - Colorado

May 16, 2025

Contributions By: US ProTech

Threats – Dangerous Nation State APT groups

Russia – (FSB, SVR, GRU)

Motivation: Harm, Disrupt, Demonstrate Capability to Adversaries.

Capability: Extremely Capable & Mature / Near Peer

Demonstrated Ability:

- Remotely compromise ICS control systems, hardware and software across critical infrastructure.
- Cyber espionage and disruptive operations

China – (PRC, CCP, PLA)

Motivation: Espionage

Capability: Highly Capable & Sophisticated / Near Peer

Demonstrated Ability:

- Conducting cyber attacks that cause localized, temporary disruptive effects on critical infrastructure – such as disrupting natural gas pipelines for days/weeks
- Intellectual property theft

Iran – (IRGC, Proxy Groups)

Motivation: Attack & Destroy

Capability: Increasing Sophistication

Demonstrated Ability:

Offensive Cyber fully integrated into Tehran’s national security

- “Eye for an eye” approach in responding to attacks
- Sabotage, influence operations & disruption

N. Korea – (DPRK, RGB)

Motivation: Generate Revenue & Espionage

Capability: Increasing Sophistication

Demonstrated Ability:

Remains a cyber espionage threat; conducts disruptive, destructive cyber attacks.

- Cyber operations previously supported regime priorities.
- Cyber crime, financial and destruction

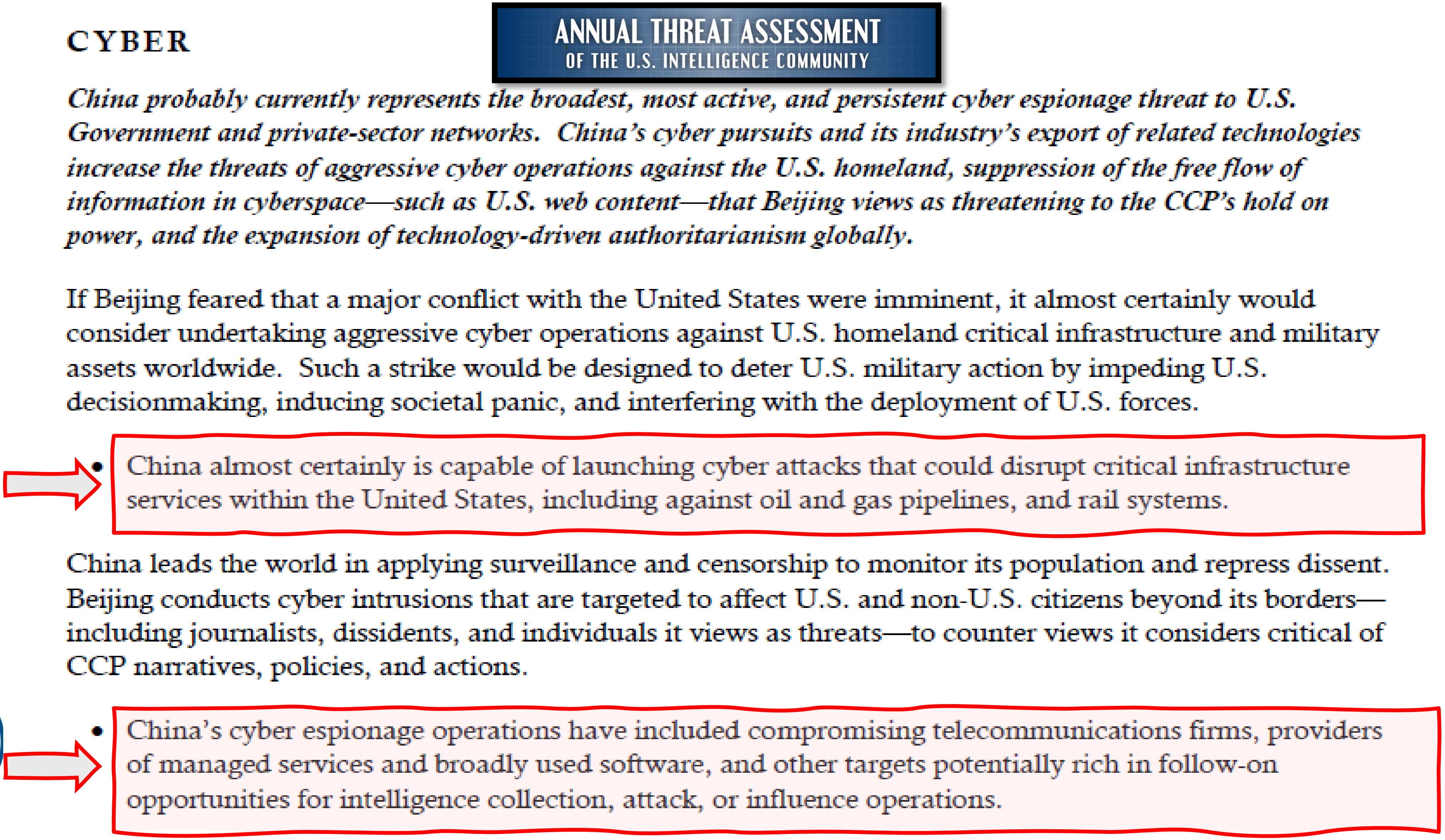
CHINA’s Strategy

We should make use of the intellectual resources of other countries… We should not be reluctant to spend money on recruiting foreigners… It is a matter of strategic importance.

—Deng Xiaoping, 1983

China consistent threat since 2019

https://www.odni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf



ANNUAL THREAT ASSESSMENT
OF THE U.S. INTELLIGENCE COMMUNITY

CYBER

China probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks. China's cyber pursuits and its industry's export of related technologies increase the threats of aggressive cyber operations against the U.S. homeland, suppression of the free flow of information in cyberspace—such as U.S. web content—that Beijing views as threatening to the CCP's hold on power, and the expansion of technology-driven authoritarianism globally.

If Beijing feared that a major conflict with the United States were imminent, it almost certainly would consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide. 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.

- China almost certainly is capable of launching cyber attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems.

China leads the world in applying surveillance and censorship to monitor its population and repress dissent. Beijing conducts cyber intrusions that are targeted to affect U.S. and non-U.S. citizens beyond its borders—including journalists, dissidents, and individuals it views as threats—to counter views it considers critical of CCP narratives, policies, and actions.

- China's cyber espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations.

PRC Threat: Volt Typhoon

Volt Typhoon

Also Known By:

- BRONZE SILHOUETTE
- Vanguard Panda
- Insidious Taurus
- DEV-0391
- UNC3236
- Voltzite
- Redfly

Volt Typhoon is a People’s Republic of China (PRC) state sponsored APT group that focuses on stealthy and targeted cyber espionage campaigns against critical infrastructure sectors.

There are multiple publicly disclosed Typhoon threat actor groups (*Volt, Flax, Salt, Silk, Granite, …).*

CISA Publications Related to PRC Threat

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.

This advisory from the United States National Security Agency (NSA), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Federal Bureau of Investigation (FBI), the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the Communications Security Establishment's Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), and the United Kingdom National Cyber Security Centre (NCSC-UK) (hereafter referred to as the "authoring agencies") provides an overview of hunting guidance and associated best practices to detect this activity.

One of the actor's primary tactics, techniques, and procedures (TTPs) is living off the land, which uses built-in network administration tools to perform their objectives. This TTP allows the actor to evade detection by blending in with normal Windows system and network activities, avoid endpoint detection and response (EDR) products that would alert on the introduction of third-party applications to the host, and limit the amount of activity that is captured in default logging configurations. Some of the built-in tools this actor uses are: `wmic`, `ntdsutil`, `netsh`, and `PowerShell`. The advisory

Disclaimer: This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp/.

TLP:CLEAR

U/OO/156893-23 | PP-23-1143 | JUN 2023 Ver. 1.1

JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA24-038A

February 7, 2024

ASD Australian Signals Directorate
ACSC

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

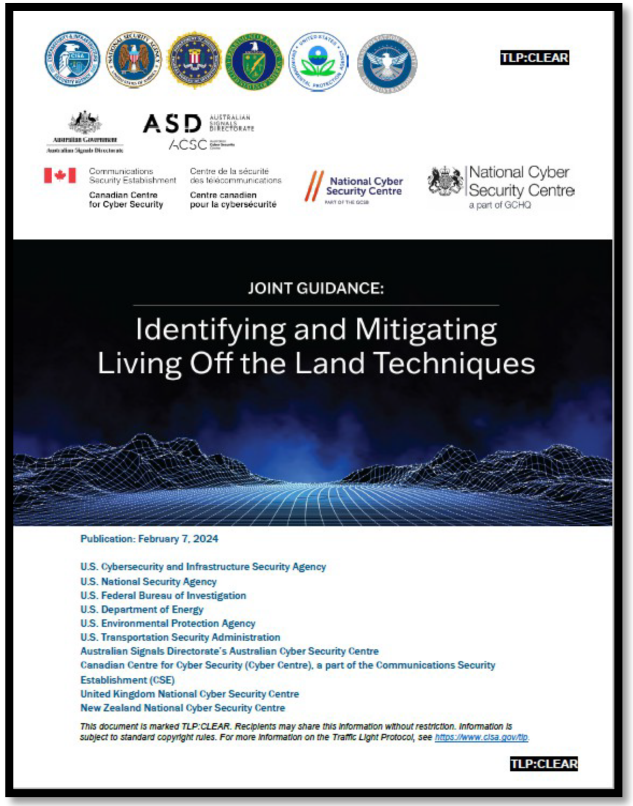
National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

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

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

TLP:CLEAR



TLP:CLEAR

Australian Government
Australian Signals Directorate

ASD Australian Signals Directorate
ACSC

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

JOINT GUIDANCE:

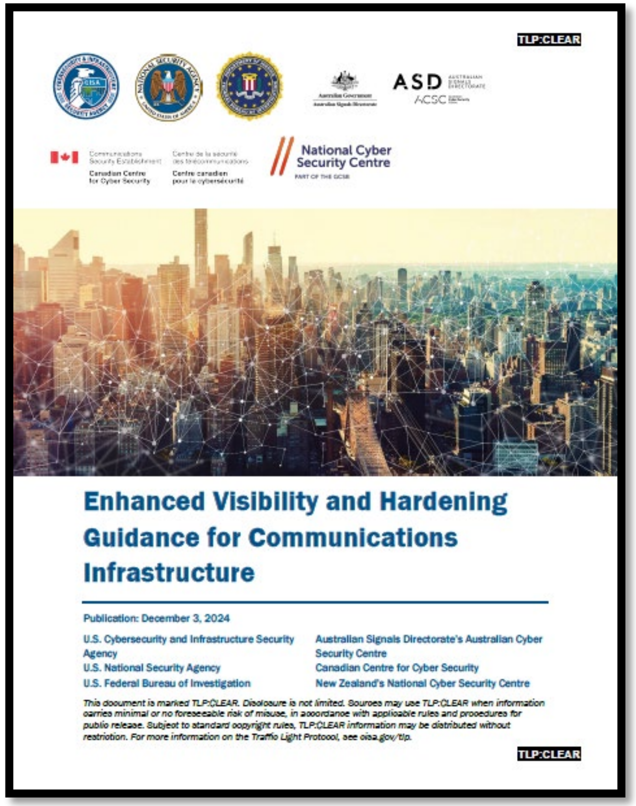
Identifying and Mitigating Living Off the Land Techniques

Publication: February 7, 2024

U.S. Cybersecurity and Infrastructure Security Agency
U.S. National Security Agency
U.S. Federal Bureau of Investigation
U.S. Department of Energy
U.S. Environmental Protection Agency
U.S. Transportation Security Administration
Australian Signals Directorate's Australian Cyber Security Centre
Canadian Centre for Cyber Security (Cyber Centre), a part of the Communications Security Establishment (CSE)
United Kingdom National Cyber Security Centre
New Zealand National Cyber Security Centre

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

TLP:CLEAR



TLP:CLEAR

Australian Government
Australian Signals Directorate

ASD Australian Signals Directorate
ACSC

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

Enhanced Visibility and Hardening Guidance for Communications Infrastructure

Publication: December 3, 2024

U.S. Cybersecurity and Infrastructure Security Agency
U.S. National Security Agency
U.S. Federal Bureau of Investigation

Australian Signals Directorate's Australian Cyber Security Centre
Canadian Centre for Cyber Security
New Zealand's National Cyber Security Centre

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

TLP:CLEAR

Observed Target Sectors: Communications, IT, Energy, Water, Transportation

https://www.cisa.gov/china

How did we get here?

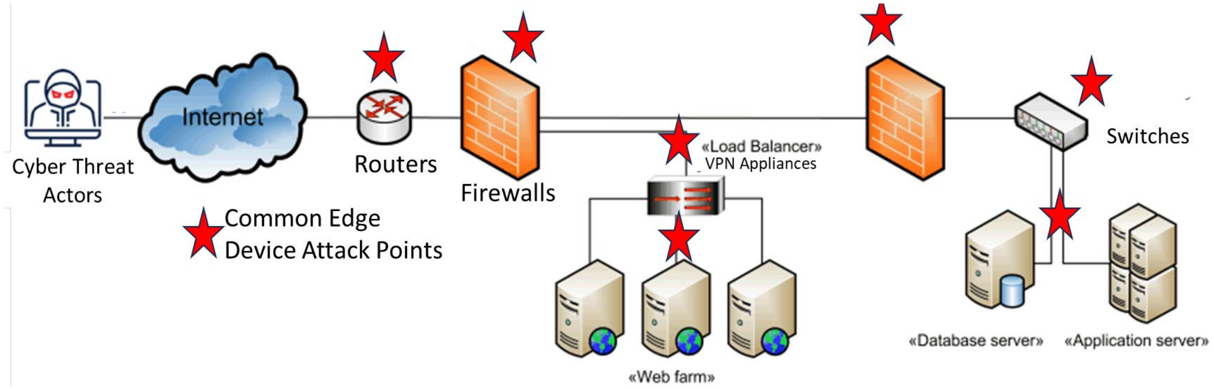
How industry evolved in response to threats

Past PRC TTPs	Industry Response
Initial Intrusion: Spearfishing	Email security tools, sandboxing links
Persistence: Unique Malware	Malware analysis and IOC sharing
C2: Consistent and finger-printable	Infrastructure pattern recognition

How threat evolved in response to industry

Past PRC TTPs

- Initial Intrusion: Spearfishing
- Persistence: Unique Malware
- C2: Consistent and finger-printable



Current PRC TTPs

- ★ Initial intrusion: edge device / supply chain exploit
- Establish persistence: credential harvesting
- C2 Channels: unique and hard to find.
- Lateral movement: LOLbins or existing infrastructure

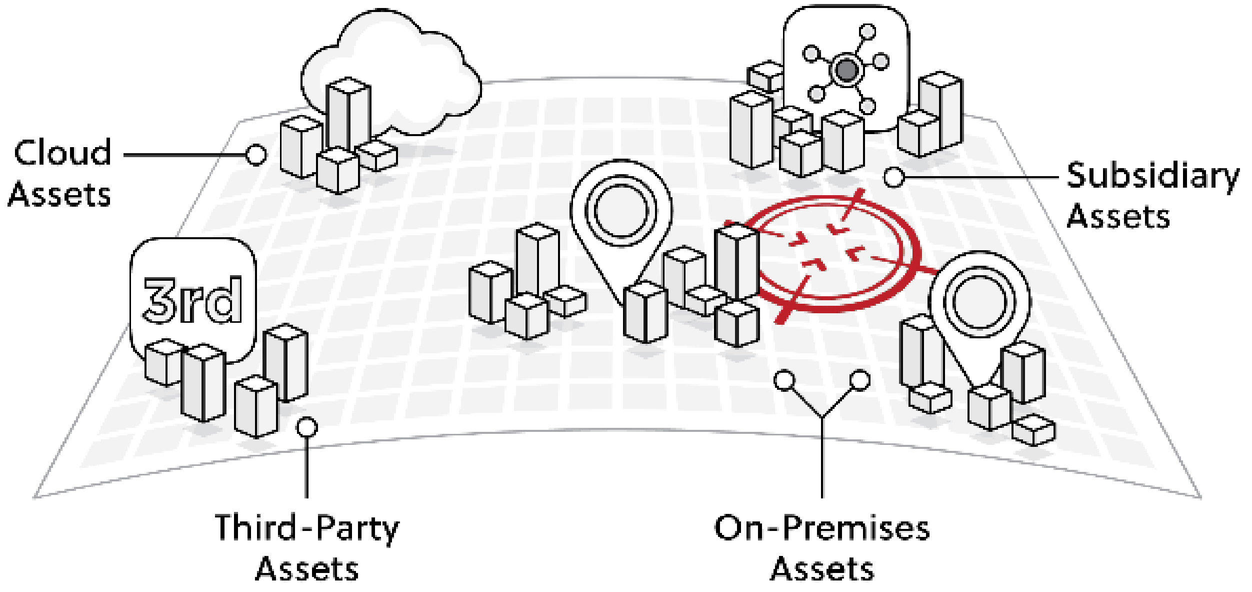
Living off the land – what is it?

LOLBins – Attackers leverage existing tools to carry out their malicious activities

- ✓ WMIC
- ✓ PowerShell
- ✓ AD Tools
- ✓ PSExec
- ✓ RDP
- ✓ Built In Tools

Offers the attacker

- Evade detection
- Avoid endpoint detection and response (EDR)
- Limit amount of activity seen by defenders



YOUR ATTACK SURFACE

The Typhoons – Attack Vectors

SOPHOS
Firewall

- CVE-2022-3236

FORTINET

- CVE-2022-42475
- CVE-2024-21762

paloalto
NETWORKS

- CVE-2024-3400

FortiClient VPN
Remote Access Agent

- CVE-2023-48788
- CVE-2024-55591

ManageEngine
a division of Zoho Corp.

- CVE-2021-40539

Exchange

- CVE-2021-26855
- CVE-2021-26857
- CVE-2021-26858
- CVE-2021-27065

ivanti
Connect Secure

- CVE-2023-46805
- CVE-2024-21887
- CVE-2025-22457
- CVE-2025-0282

CISCO

- CVE-2018-0171
- CVE-2023-20198
- CVE-2023-20273

CITRIX

- CVE-2023-6548
- CVE-2023-6549
- CVE-2023-3519

Attack Walkthrough

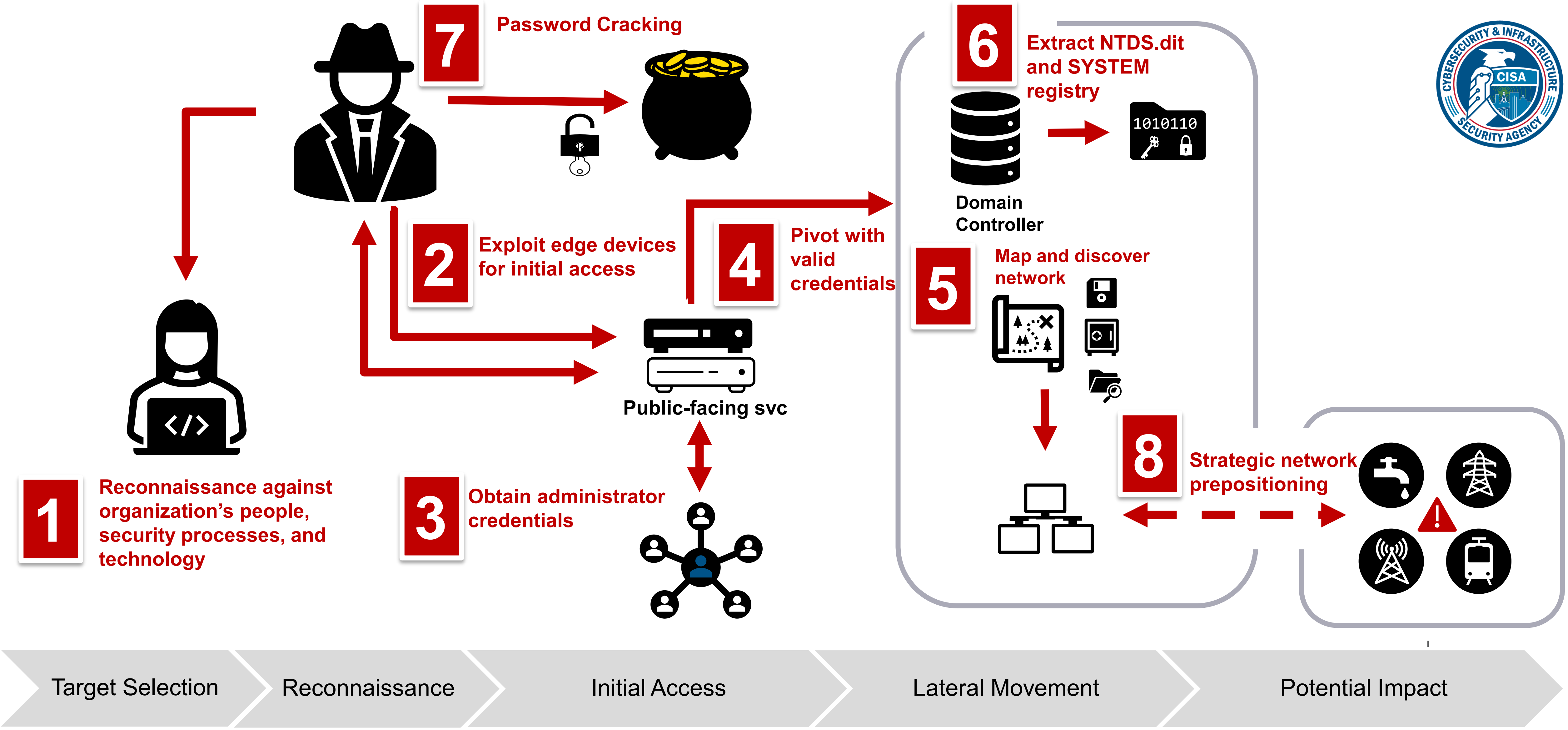
Volt Typhoon Activity

Volt Typhoon is a sophisticated People’s Republic of China (PRC) state-sponsored cyber threat actor group that targets US Critical Infrastructure (CI).

Volt Typhoon follows a **five-step attack plan** when targeting US Critical Infrastructure.

1. Target Selection
2. Reconnaissance
3. Initial Access
4. Lateral Movement
5. Potential Impact

Volt Typhoon Activity – Case Example



1 Reconnaissance against organization’s people, security processes, and technology

2 Exploit edge devices for initial access

3 Obtain administrator credentials

4 Pivot with valid credentials

5 Map and discover network

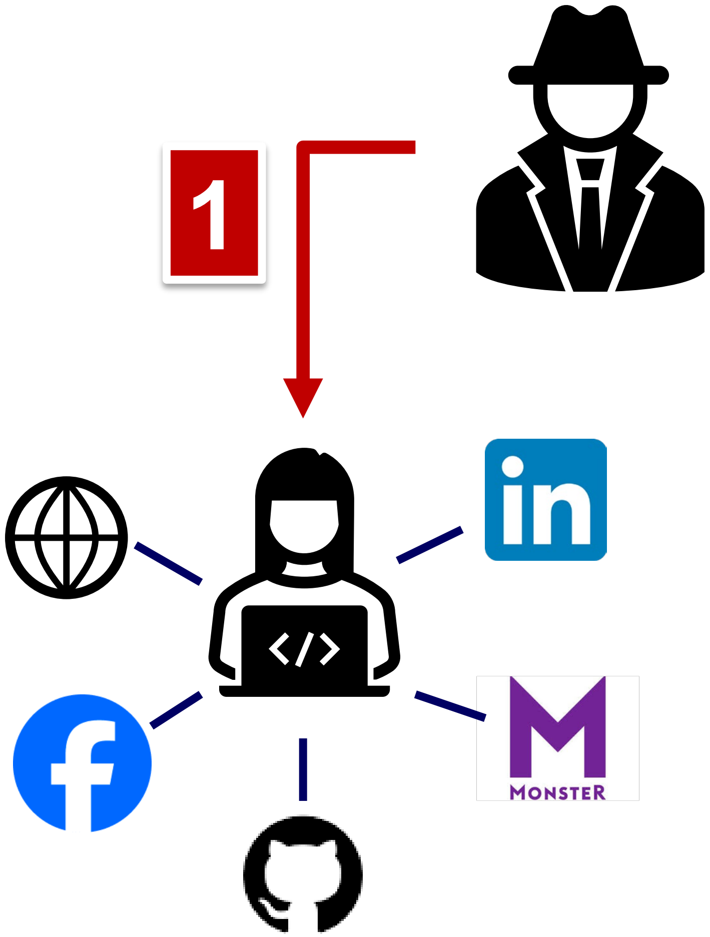
6 Extract NTDS.dit and SYSTEM registry

7 Password Cracking

8 Strategic network prepositioning

Target Selection → Reconnaissance → Initial Access → Lateral Movement → Potential Impact

Reconnaissance

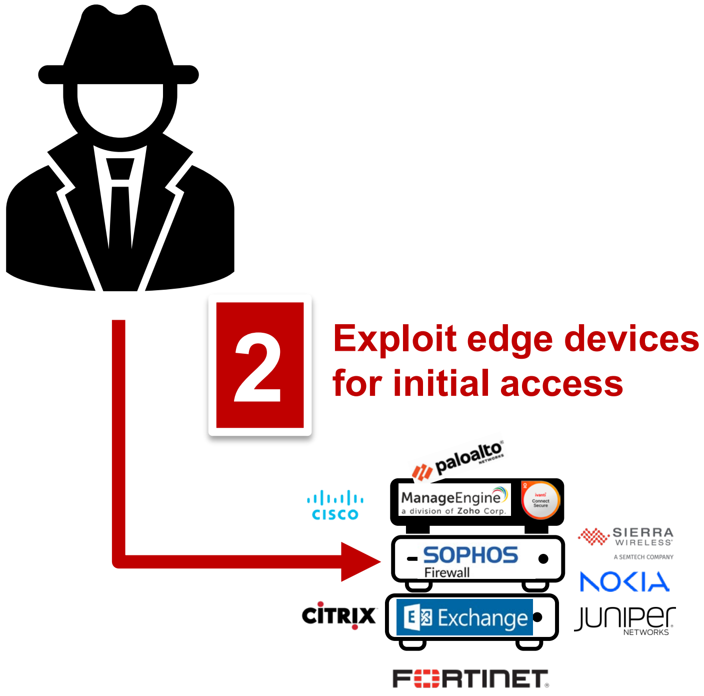


What information are you sharing?

- LinkedIn
- Job postings
- GitHub
- Facebook
- Websites
- Business Journals

Target Selection | **Reconnaissance** | Initial Access | Lateral Movement | Potential Impact

Initial Access



2 Exploit edge devices for initial access

Mitigation - Start with the Basics!

- Identify - block and disable unnecessary edge services
- Limit remote access through VPN or gateways
- Enable logging on edge devices
- Require Multi-Factor Authentication
- Secure configuration of edge devices
  - CyHy | WAS
- Secure Configuration of Cloud Devices
  - SCUBA

SHODAN

censys

FOFA

Qualys.

Volt Typhoon actors typically obtain initial access through commonly exploited vulnerabilities, misconfigured edge devices or use valid credentials.

CISA Cyber Hygiene Services

Vulnerability Scanning
Web Application Scanning

CISA CYBER+INFRASTRUCTURE

ScubaGear
ScubaGoggles

Available at https://github.com/cisagov

Target Selection | Reconnaissance | **Initial Access** | Lateral Movement

Privilege Escalation and Lateral Movement

3

Obtain administrator credentials

- Exploit and execute privilege escalation vulnerabilities on host
- Extract insecurely stored credentials on public facing appliance.
- Dump passwords from host operating system

4

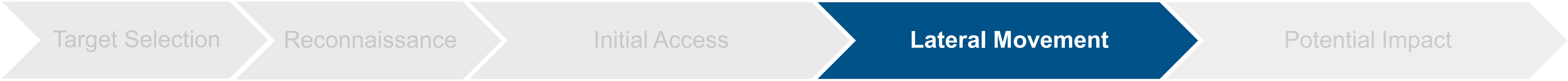
Pivot with modified User or Group modified valid credentials

- Remote Desktop Protocol | Terminal Services
- PSExec
- Putty
- SSH
- API keys…

5

Map and discover network

- PowerShell – targeted queries on event logs
- WMIC



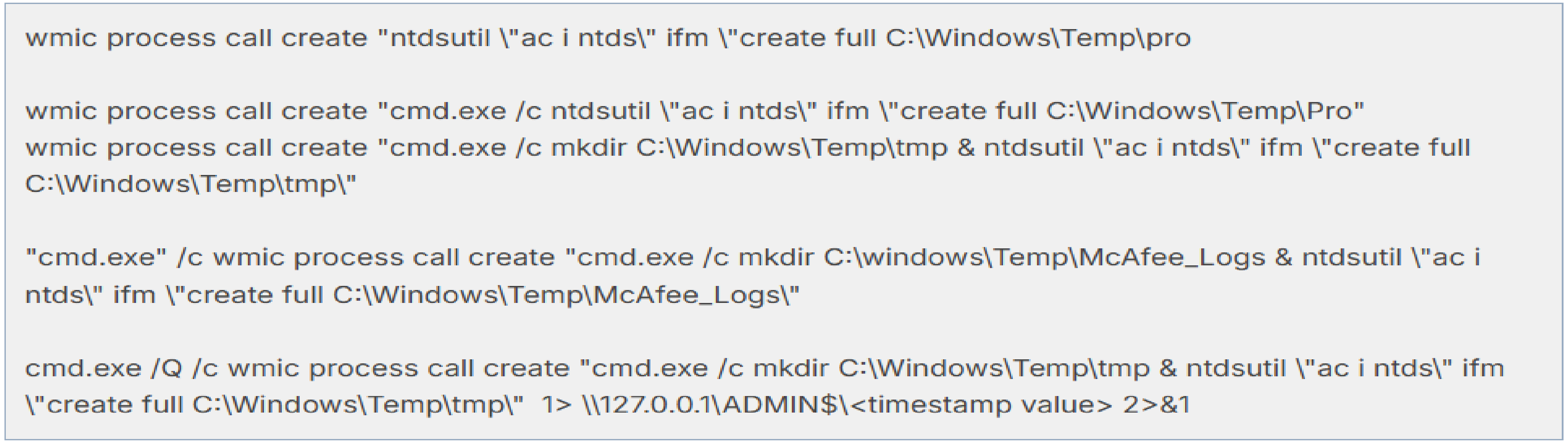
Obtain Credentials NTDS.dit Extraction

Significance:

- Attacker gains access to every NT hash in domain
- Extracted hashes can be cracked or used in pass-the-hash attacks.
- Opens door to Golden Ticket attacks & persistent DA access

Extraction Techniques:

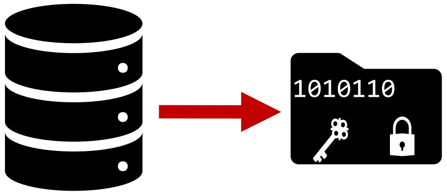
- Volume Shadow Copy of the NTDS.dit file



```
wmic process call create "ntdsutil \"ac i ntds\" ifm \"create full C:\Windows\Temp\pro

wmic process call create "cmd.exe /c ntdsutil \"ac i ntds\" ifm \"create full C:\Windows\Temp\Pro"
wmic process call create "cmd.exe /c mkdir C:\Windows\Temp\tmp & ntdsutil \"ac i ntds\" ifm \"create full
C:\Windows\Temp\tmp\"

"cmd.exe" /c wmic process call create "cmd.exe /c mkdir C:\windows\Temp\McAfee_Logs & ntdsutil \"ac i
ntds\" ifm \"create full C:\Windows\Temp\McAfee_Logs\"

cmd.exe /Q /c wmic process call create "cmd.exe /c mkdir C:\Windows\Temp\tmp & ntdsutil \"ac i ntds\" ifm
\"create full C:\Windows\Temp\tmp\"  1> \\127.0.0.1\ADMIN$\<timestamp value> 2>&1
```

- The SYSKEY is extracted from the registry to decrypt the data contained in NTDS.dit

Extracting NTDS.dit and SYSTEM registry



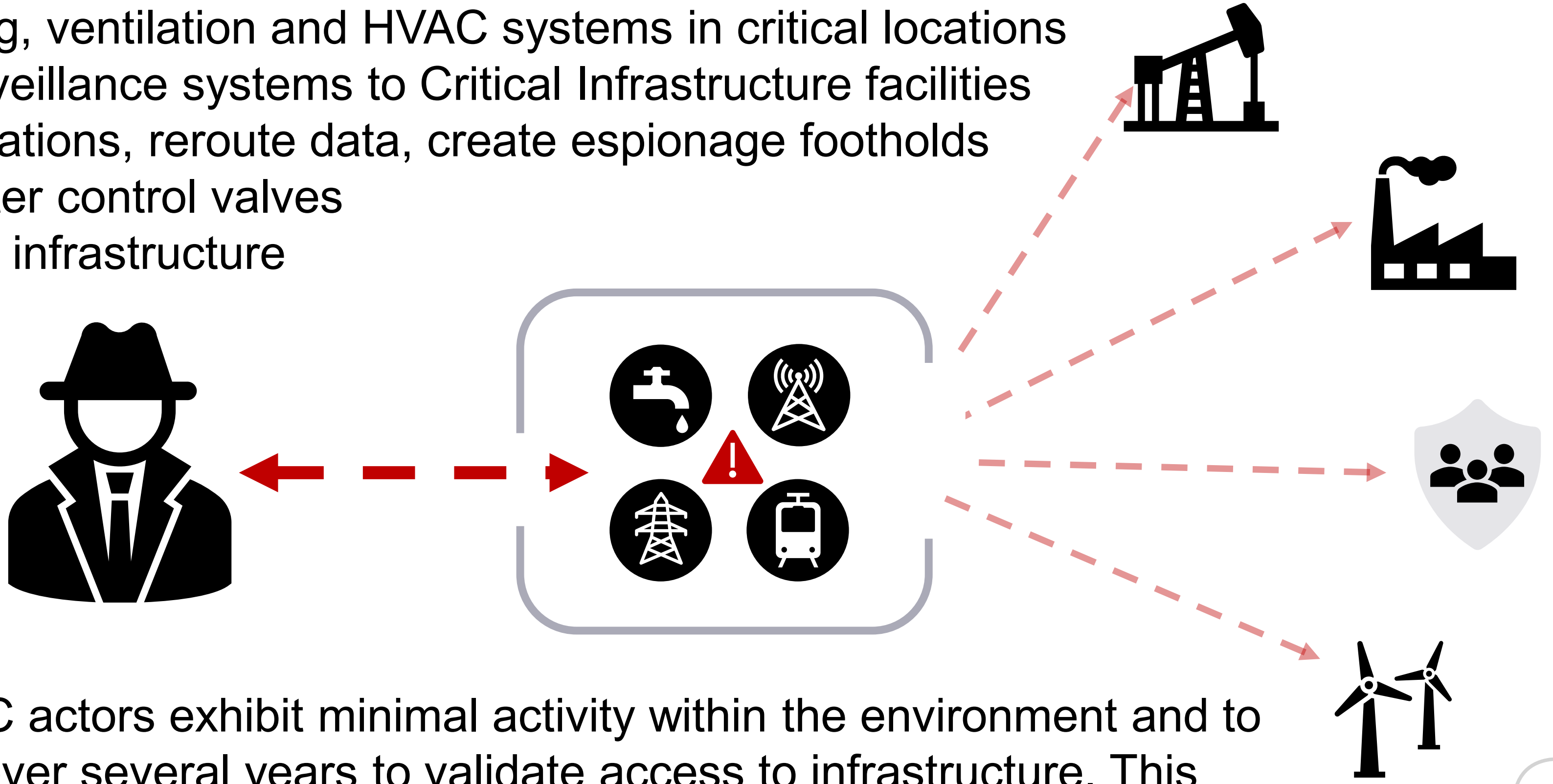
Domain Controller

Operational Environment – Access & Persist

8

Gain Access to Operational Environment

- Manipulating heating, ventilation and HVAC systems in critical locations
- Access camera surveillance systems to Critical Infrastructure facilities
- Intercept communications, reroute data, create espionage footholds
- Open and close water control valves
- Manipulate physical infrastructure

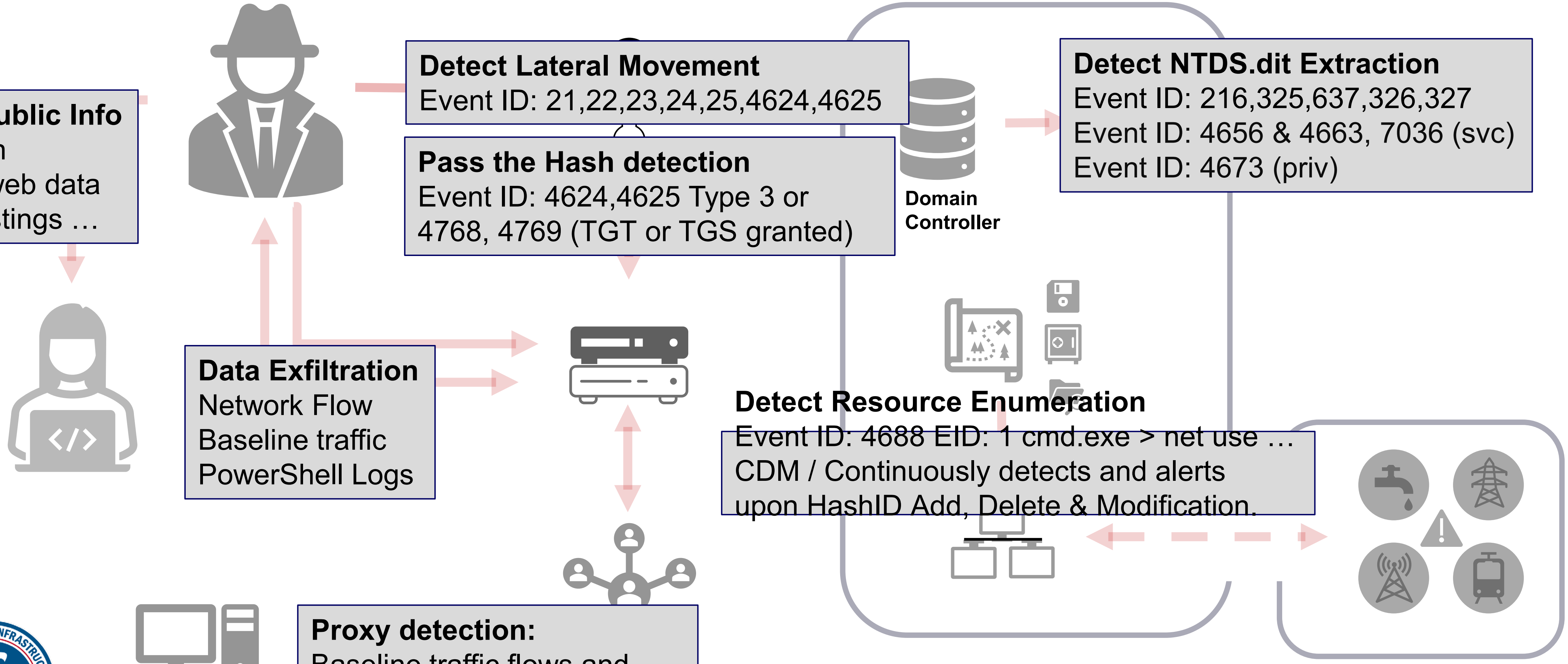


After exploitation – PRC actors exhibit minimal activity within the environment and to re-target environment over several years to validate access to infrastructure. This activity suggesting their objective is to maintain persistence rather than immediate exploitation

Target Selection | Reconnaissance | Initial Access | Lateral Movement | **Potential Impact**

Detection & Mitigation Guidance

Detection is possible … if you look for it!



Limit Public Info
LinkedIn
Public web data
Job Postings …

Detect Lateral Movement
Event ID: 21,22,23,24,25,4624,4625

Pass the Hash detection
Event ID: 4624,4625 Type 3 or
4768, 4769 (TGT or TGS granted)

Detect NTDS.dit Extraction
Event ID: 216,325,637,326,327
Event ID: 4656 & 4663, 7036 (svc)
Event ID: 4673 (priv)

Data Exfiltration
Network Flow
Baseline traffic
PowerShell Logs

Detect Resource Enumeration
Event ID: 4688 EID: 1 cmd.exe > net use …
CDM / Continuously detects and alerts
upon HashID Add, Delete & Modification.

Proxy detection:
Baseline traffic flows and
Uncommon data patterns.
Know normal communication

Detection – Logging Vs. HashID Analytics

Centralized Logging Vs. Host Based Forensics

- Implement Security Information and Event Management (SIEM)
- Logging / Network Based SIEM - verbose logging and aggregate logs in an out-of-band centralized location.
    - Increase log retention (hot, warm, cold) – what is your minimum?
    - Options: Splunk, QRadar, Securonix, Etc.
- Forensics / System Based SIEM - comprehensive comparative HashID Analytics directly from Host or System
    - Gain automated visibility and real-time continuous risk assessment into IoA's, Ioc's, ZDE's, and CVE's.
    - Monitor Users, Groups, Ports, Permissions, and Transactions at a forensic level, 24/7 without data entry.
    - Options: ANAMO CDM
- Volt Typhoon – extended dwell time (5 years)
- Fine-tune log alerts and utilize CDM to reduce noise.
- Test your playbooks
- **Perform Log Analysis and HashID Analytics to hunt for PRC threats and Technical Adversaries**

Log Analysis – Key events to Look for

Key Event Log Indicators:

- Event ID 216: Detecting changes in NTDS.dit database location
- Event ID 325: Creation of a new NTDS.dit database in unusual directories
- Event ID 637: Generation of a new flush map file for NTDS.dit
- Event ID 326: Mounting of NTDS.dit file from a shadow copy
- Event ID 327: Detachment of NTDS.dit
- Event ID 4656 & 4663: File Access Auditing SACL must be defined for ntds.dit file
- Event ID 25: (Term Services-Local Session): Successful RDP session reconnections
- Event ID 22: (Term Services-Local Session): Successful RDP Session Created
- Event ID 1017: (System Log): Server handle closures in unusual patterns/locations
- Event ID 1102: (Security Log): Security Logs Cleared
- Event ID 4624: (Security Log): Successfully Logged on (type 10: RemoteInteractive)
- Event ID 4688: (Security Log): A new process has been created

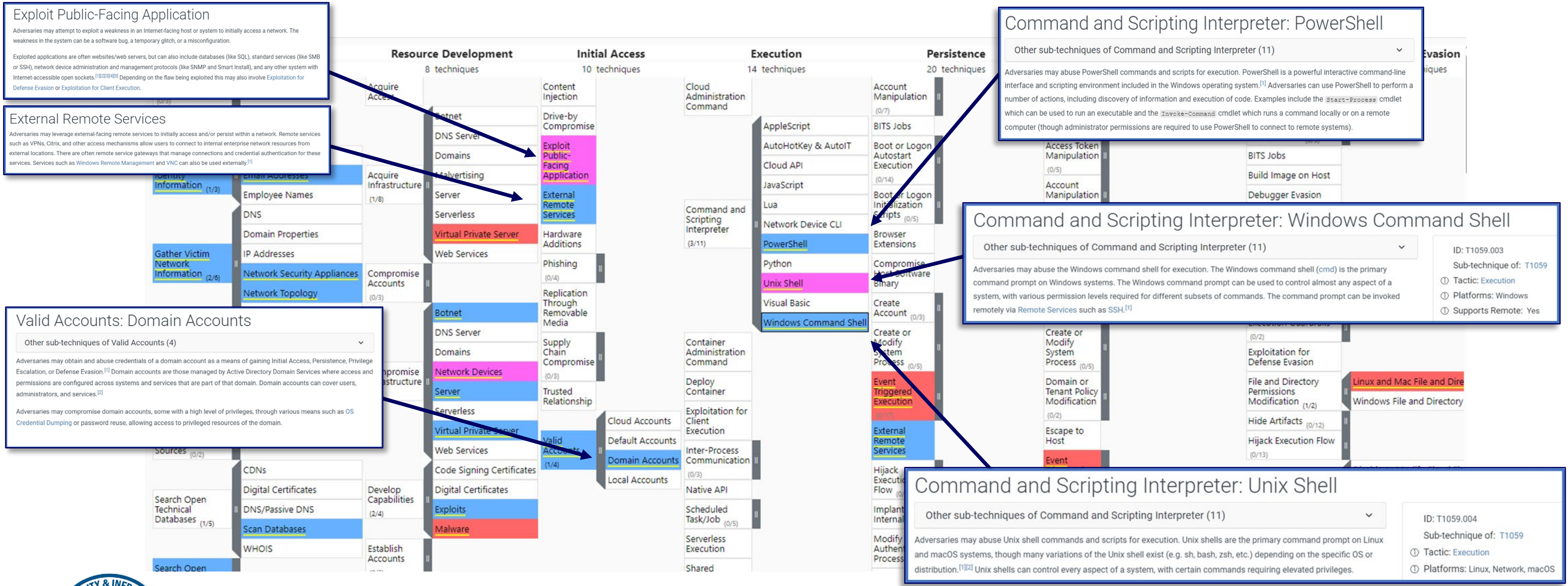
Detection Opportunities

- **Leverage "CDM" Continuous, Diagnostics & Mitigation (such as ANAMO CDM)**
- **https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program**
- **Suspicious PowerShell Use or Unusual Command Shall Acticvity:**
  - Monitor for commands such as *Get-EventLog security* – Event ID 4624 used to identify successful logons.
- **NTDS Dumping:**
  - Look for attempts to access or copy the ntds.dit file using commands like *ntdsutil* or *vssadmin* create shadow.
- **Event Log Monitoring:**
  - Event ID 4688: Enable logging of command line process creation to capture detailed command line activities.
  - Event ID 1102: Investigate all log clearing activities
- **PortProxy Usage:**
  - Detect the use of netsh interface portproxy commands to create unauthorized port forwarding rules (e.g., *netsh interface portproxy add v4tov4 listenport*=..., Fast Reverse Proxy, Earth Worm).
- **Cross-zone Communications:**
  - Monitor for communications between IT and OT networks or other segments.
- **Leverage Sysmon and Host-based Logs:**
  - Sysmon logs provide visibility into system activities, offering a detailed record of process creations, network connections, registry modifications, cryptographic hashes, and more

Harden the Attack Surface

- **Allocate time and Resources:** Internal Threat Hunting – be proactive instead of reactive.
- **Vulnerability Scanning: Automated Continuously 24/7 Using ANAMO.** Or, Manually interrogate External networks weekly, Internal networks monthly (Free Cyber Hygiene Services)
- **Patching Internet-Facing Systems:** Edge devices are actively exploited for initial access – Zero-day vulnerabilities – Average time to exploit 5-days. Continuously monitor IoA's, IoC's and ZDE's 24/7 with ANAMO.
- **Software and System Hardening:** Applying vendor-provided or industry-standard hardening guides.
- **Tailored Mitigations for Volt Typhoon:** Behavior analytics, anomaly detection, and proactive hunting as part of a comprehensive security approach – 3rd party assessments.
- **Secure Credentials** - Unique passwords, eliminate group or shared accounts – group managed service accounts
- **Separation of User and Privileged Accounts:** Separate accounts for user and admin functions. PAWs
- **Privileged Access Management (PAM) Solutions: Continuously monitor 24/7 with ANAMO.** Consider PAM solutions for managing access to privileged accounts, including logging and alerting unusual activity.
- **Secure Remote Access & Sensitive Data:** Limit remote access to where it’s needed and audit access
- **Network Segmentation:** Segment IT and OT environments and further isolate IT network to improve security.

Detection is possible … if you look for it!



Exploit Public-Facing Application

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.

Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet-accessible open sockets.[1][2][3][4][5] Depending on the flaw being exploited this may also involve Exploitation for Defense Evasion or Exploitation for Client Execution.

External Remote Services

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management and VNC can also be used externally.[1]

Valid Accounts: Domain Accounts

Other sub-techniques of Valid Accounts (4) ⌄

Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.[1] Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover users, administrators, and services.[2]

Adversaries may compromise domain accounts, some with a high level of privileges, through various means such as OS Credential Dumping or password reuse, allowing access to privileged resources of the domain.

Command and Scripting Interpreter: PowerShell

Other sub-techniques of Command and Scripting Interpreter (11) ⌄

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.[1] Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems).

Command and Scripting Interpreter: Windows Command Shell

Other sub-techniques of Command and Scripting Interpreter (11) ⌄

Adversaries may abuse the Windows command shell for execution. The Windows command shell (cmd) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via Remote Services such as SSH.[1]

ID: T1059.003
Sub-technique of: T1059
ⓘ Tactic: Execution
ⓘ Platforms: Windows
ⓘ Supports Remote: Yes

Command and Scripting Interpreter: Unix Shell

Other sub-techniques of Command and Scripting Interpreter (11) ⌄

Adversaries may abuse Unix shell commands and scripts for execution. Unix shells are the primary command prompt on Linux and macOS systems, though many variations of the Unix shell exist (e.g. sh, bash, zsh, etc.) depending on the specific OS or distribution.[1][2] Unix shells can control every aspect of a system, with certain commands requiring elevated privileges.

ID: T1059.004
Sub-technique of: T1059
ⓘ Tactic: Execution
ⓘ Platforms: Linux, Network, macOS

ATT&CK® Navigator Overlay for Volt Typhoon

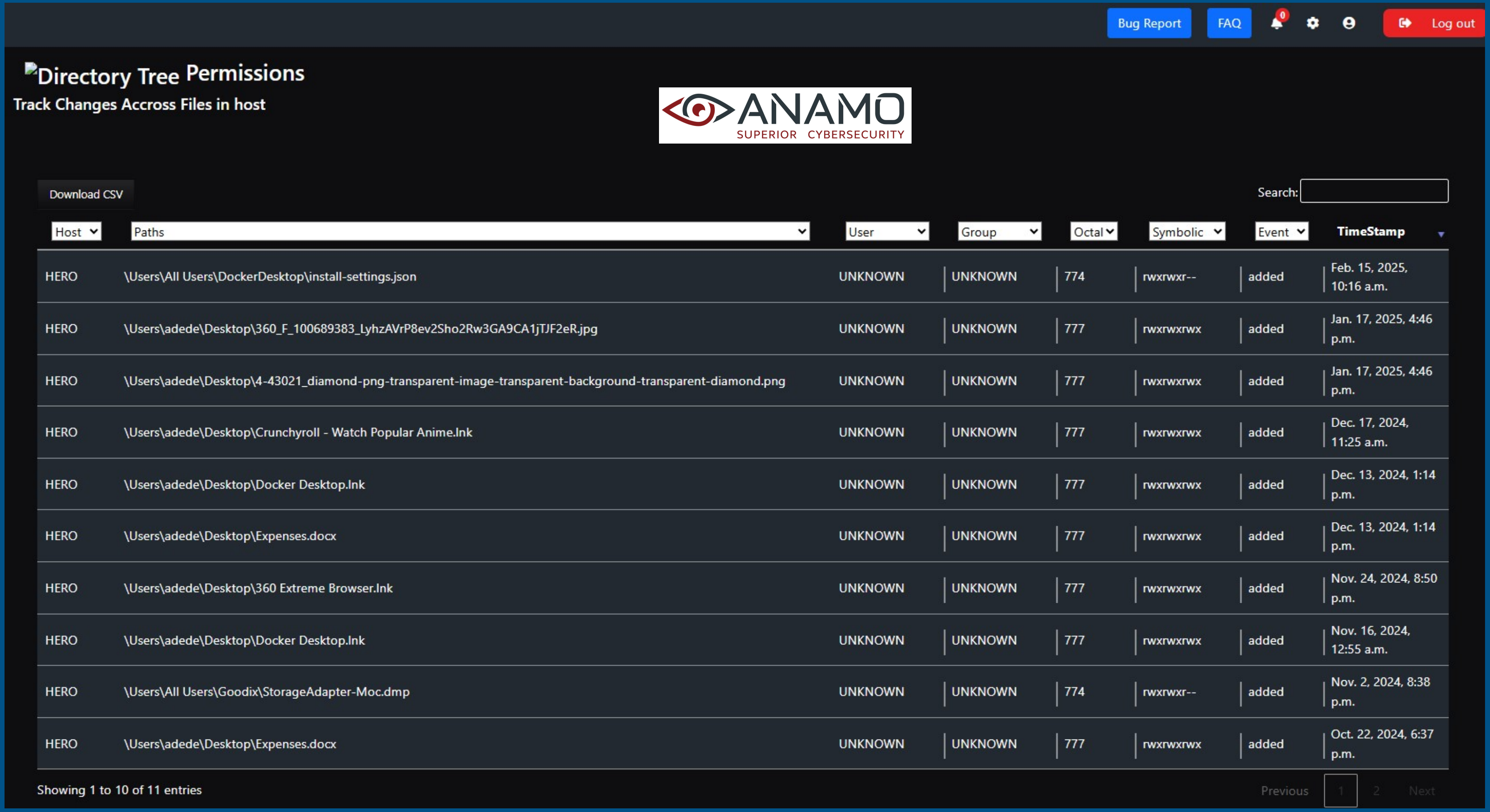
“Prevention is ideal, but detection is a must.”

- Dr. Eric Cole (SANS)

What if you could....

Know who has what Permission on which Device Anywhere and at Anytime, and at the same time Forensically track every Permission modification on every device with automatic alert notifications by tracking Comparative HashID Analytics?

If so, Contact US ProTech and ask to see Anamo CDM, today!



Directory Tree Permissions

Track Changes Accross Files in host

Host	Paths	User	Group	Octal	Symbolic	Event	TimeStamp
HERO	\Users\All Users\DockerDesktop\install-settings.json	UNKNOWN	UNKNOWN	774	rwxrwxr--	added	Feb. 15, 2025, 10:16 a.m.
HERO	\Users\adede\Desktop\360_F_100689383_LyhzAVrP8ev2Sho2Rw3GA9CA1jTJF2eR.jpg	UNKNOWN	UNKNOWN	777	rwxrwxrwx	added	Jan. 17, 2025, 4:46 p.m.
HERO	\Users\adede\Desktop\4-43021_diamond-png-transparent-image-transparent-background-transparent-diamond.png	UNKNOWN	UNKNOWN	777	rwxrwxrwx	added	Jan. 17, 2025, 4:46 p.m.
HERO	\Users\adede\Desktop\Crunchyroll - Watch Popular Anime.lnk	UNKNOWN	UNKNOWN	777	rwxrwxrwx	added	Dec. 17, 2024, 11:25 a.m.
HERO	\Users\adede\Desktop\Docker Desktop.lnk	UNKNOWN	UNKNOWN	777	rwxrwxrwx	added	Dec. 13, 2024, 1:14 p.m.
HERO	\Users\adede\Desktop\Expenses.docx	UNKNOWN	UNKNOWN	777	rwxrwxrwx	added	Dec. 13, 2024, 1:14 p.m.
HERO	\Users\adede\Desktop\360 Extreme Browser.lnk	UNKNOWN	UNKNOWN	777	rwxrwxrwx	added	Nov. 24, 2024, 8:50 p.m.
HERO	\Users\adede\Desktop\Docker Desktop.lnk	UNKNOWN	UNKNOWN	777	rwxrwxrwx	added	Nov. 16, 2024, 12:55 a.m.
HERO	\Users\All Users\Goodix\StorageAdapter-Moc.dmp	UNKNOWN	UNKNOWN	774	rwxrwxr--	added	Nov. 2, 2024, 8:38 p.m.
HERO	\Users\adede\Desktop\Expenses.docx	UNKNOWN	UNKNOWN	777	rwxrwxrwx	added	Oct. 22, 2024, 6:37 p.m.

Showing 1 to 10 of 11 entries

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

Any Questions or Comments?

For Additional Information On Eliminating

"Unauthorized Privileged Account Escalation"

Contact:

US ProTech, Inc. | ANAMO CDM

www.USProTech.com | https://anamo.io/

949.629.3900 | Info@ANAMO.io

Certified Cybersecurity Experts