CISA Analysis: Fiscal Year 2023 Risk and Vulnerability Assessments

Publication: September 2024

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

RISK AND VULNERABILITY ASSESSMENTS

The Cybersecurity and Infrastructure Security Agency (CISA) conducts Risk and Vulnerability Assessments (RVAs) for the federal civilian executive branch (FCEB), high priority private and public sector critical infrastructure (CI) operators, and select state, local, tribal, and territorial (SLTT) stakeholders. Concurrently, the United States Coast Guard (USCG) conducts RVAs on maritime CI operated by SLTT and private-sector organizations.

The RVA is intended to assess the entity's network capabilities and network defenses against known threats. In Fiscal Year 2023 (FY23), CISA and the USCG conducted a combined total of **143** RVAs across multiple CI sectors.[1] Each RVA maps the results to the MITRE ATT&CK® framework, which includes 14 tactics, techniques, and procedures (TTPs) that cyber threat actors use to obtain and maintain unauthorized access to a network or system. The 143 RVAs map to 11 of the 14 tactics. The goal of the RVA analysis is to develop effective strategies to improve the security posture of FCEB, CI, maritime, and SLTT stakeholders.

During each RVA, CISA and the USCG collect data through remote and onsite actions. This data is combined with national threat and vulnerability information to provide organizations with actionable remediation recommendations prioritized by risk of compromise. CISA designed RVAs to identify vulnerabilities threat actors could exploit to compromise network security controls. After completing an RVA, CISA and the USCG provide the assessed entity a final report that includes recommendations, specific findings, potential mitigations, and technical attack path details.

The FY23 reports provided these general observations:

- Assessors completed their most successful attacks via common methods, such as phishing, valid accounts, and default credentials.
- Assessors used a variety of tools and techniques CISA has captured in previous RVA analyses to successfully conduct common attacks.
- Many organizations across varying CI sectors exhibited the same vulnerabilities.
- CISA assessment personnel used common vulnerabilities facilitated by shortcomings in secure by design and default principles and other misconfigurations to compromise systems.

ATTACK PATH ANALYSIS

This report analyzes a sample attack path cyber threat actors could leverage to compromise an organization using weaknesses identified in the FY23 RVAs. CISA and the USCG developed the sample attack path based loosely on 11 of the MITRE ATT&CK framework's 14 tactics. Although the sample attack path does not encompass all the potential steps threat actors could use—and not all attack paths follow this model—a skilled threat actor could follow this path to successfully exploit a target. Assessment teams attempt to find the easiest and most opportunistic means of accessing the target network without interfering with dependencies that would disrupt operations. The sample attack path highlights the more successful attack strategies used during RVAs, and the impacts these strategies have on target networks.

[1] The number of assessments conducted within each sector vary and are not equivalent across all 16 sectors.

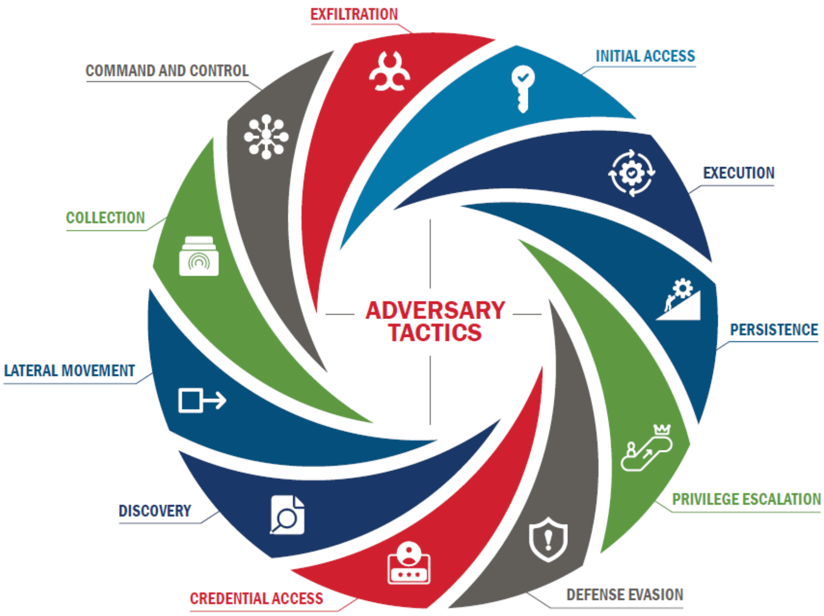

Figure 1: Adversary Tactics

The attack path begins with a step required by many real-world attacks: gaining *Initial Access* [TA0001]. Next, the attacker *Executes* [TA0002] code in the network to help establish a foothold and maintain *Persistence* [TA0003] on the network. Using the initial foothold on the network, the attacker uses *Privilege Escalation* [TA0004] to gain administrative rights. Using *Defense Evasion* [TA0005] to avoid detection, the attacker could attempt to steal credentials with *Credential Access* [TA0006]. Once the attacker has credential access, they *Discover* [TA0007] the systems and networks. By analyzing these systems and networks, the attacker gains an understanding of the infrastructure and identifies sensitive data that they deem worth compromising. The attacker then uses *Lateral Movement* [TA0008] throughout the network to access this sensitive data. Once entrenched in the network, the attacker switches their focus to *Collection* [TA0009] of the sensitive data. Attackers use *Command and Control* (C2) [TA0011] to keep communication channels open to support data *Exfiltration* [TA0010] and potential control after the attack.

Real-World Attack Paths: PRC-affiliated Threat Actors

To provide additional context to the sample attack paths, this analysis examines several People's Republic of China (PRC)-affiliated nation-state cyber threat actors to highlight real-world implications of the vulnerabilities successfully exploited during the assessments. CISA and the USCG's assessment teams use TTPs that, like PRC-affiliated espionage activities that operate with stealth to remain undetected, avoid degrading and destroying customers' networks. The PRC threat actor examples used in this analysis are named and tracked by Mandiant and in open-source reporting.

The number of active groups operating across various clusters of activity demonstrate their intent and capability in targeting government and CI sectors.

MITRE ATT&CK and Threat Actors

INITIAL ACCESS 4
APT15, APT 31, VOLT TYPHOON, AND STORM 0558 6
EXECUTION 8
VOLT TYPHOON 8
PERSISTENCE 9
VOLT TYPHOON AND UNC5174 10
PRIVILEGE ESCALATION 10
UNC4992 11
DEFENSE EVASION 12
VOLT TYPHOON 13
CREDENTIAL ACCESS 13
VOLT TYPHOON 14
DISCOVERY 14
EARTH KRAHANG AND VOLT TYPHOON 15
LATERAL MOVEMENT 16
APT15 AND VOLT TYPHOON 17
COLLECTION 18
EARTH KRAHANG 18
COMMAND AND CONTROL (C2) 18
CHAMELGANG 19
EXFILTRATION 19
UNC4841 AND APT41 20
CONCLUSION 21
REFERENCES 22

INITIAL ACCESS

WHAT

Initial Access [TA0001] is the phase of malicious activity where threat actors attempt to obtain unauthorized access to a victim's internal network. Gaining initial access to an organization's network is one of the first active steps in a successful attack. Threat actors could use techniques— such as targeted spear phishing, valid accounts and credentials, or exploiting critical vulnerabilities and weaknesses on network edge devices—to gain an initial foothold within a network. If threat actors establish initial access, they could execute other techniques-- such as privilege escalation-- to ultimately steal information, disrupt operations, or preposition for future actions on objectives. Preventing initial access should be a main goal in protecting network assets and data, both internally and externally.

HOW

Threat actors use a variety of attack paths-- such as., gaining access to valid accounts, targeted spear phishing, leveraging insecure ports or protocols, or exploiting public-facing applications-- to compromise a victim's network. RVA analyses revealed that **Valid Accounts** [T1078] were the most common successful attack technique, responsible for **41%** of successful attempts. A common technique under this tactic is cracking password hashes, which was successful in 89% of USCG assessments to access Domain Administrator accounts. Valid accounts can be accessed internal or external to the network through default or stolen administrator accounts, or former employee accounts that have not been removed from the active directory. Additionally, initial access brokers that sell exploits and valid credentials to nation-state and criminal threat actors are seen more frequently as the profits are rising for criminal activity.[2,3] Threat actors can compromise a valid administrator account if organizations do not change default passwords, or through brute force if a weak password is in place. In many cases, this attack technique is possible because the valid account allowed unauthorized users to install or execute insecure software (such as unpatched or out-of-date software) on a system or network. Figure 2 demonstrates a valid account execution.

The second most common successful attack technique used **Phishing** or **Spear phishing** [T1566]. Spear phishing is a form of social engineering in which a cyber threat actor poses as a trustworthy colleague, acquaintance, or organization to lure a victim into providing sensitive information or network access.[4] A spear phishing attack is the delivery of targeted emails containing a malicious link or attachment designed to give the cyber threat actor an entryway into the recipient's network or system. Successful spear phishing requires an attacker's malicious email to pass through network border protections and deliver malware to execute on the local host or trick users into entering their username and password on a malicious site. Host-level protection stops spear phishing attempts as they pass through network perimeter protection.

[2] Ragi et al., "Initial Access Brokers Exploit F5 & ScreenConnect," March 21, 2024, https://www.mandiant.com/resources/blog/initial-access-brokers-exploit-f5-screenconnect.

[3] 2 Sjouwerman, S., "Initial Access Brokers: The New Face of Organized Cybercrime," September 8, 2022, https://www.securitymagazine.com/articles/98405-initial-access-brokers-the-new-face-of-organized-cybercrime.

[4] "Phishing Infographic," Cybersecurity and Infrastructure Security Agency (CISA), accessed May 9, 2023, https://www.cisa.gov/sites/default/files/publications/phishing-infographic-508c.pdf.

A cyber threat actor's success rate with this type of attack depends on factors such as the perceived authenticity of the email's content and presentation, host protections (e.g., antivirus and malware detection software), and the network's boundary protection mechanisms.

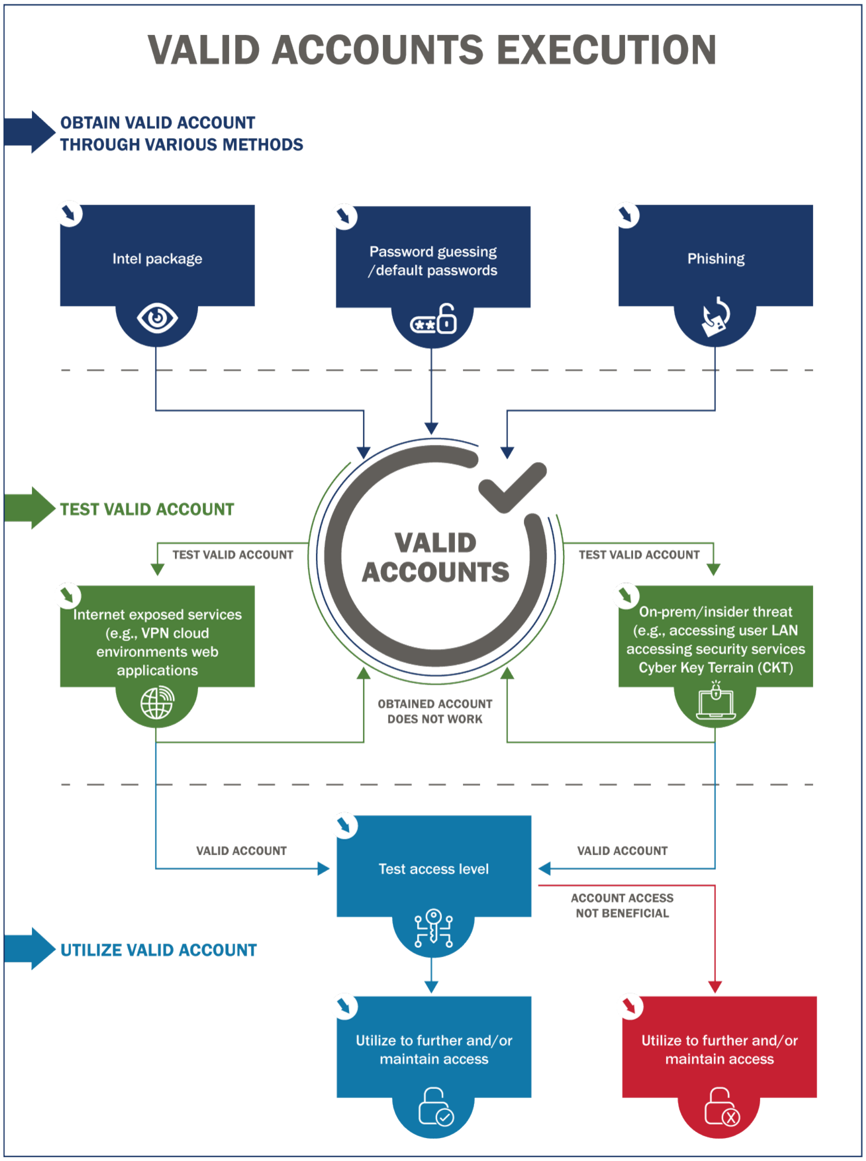
VALID ACCOUNTS EXECUTION
OBTAIN VALID ACCOUNT THROUGH VARIOUS METHODS
Intel package
Password guessing /default passwords
Phishing
TEST VALID ACCOUNT
VALID ACCOUNTS
TEST VALID ACCOUNT
TEST VALID ACCOUNT
Internet exposed services (e.g., VPN cloud environments web applications
On-prem/insider threat (e.g., accessing user LAN accessing security services Cyber Key Terrain (CKT)
OBTAINED ACCOUNT DOES NOT WORK
VALID ACCOUNT
Test access level
VALID ACCOUNT
ACCOUNT ACCESS NOT BENEFICIAL
UTILIZE VALID ACCOUNT
Utilize to further and/or maintain access
Utilize to further and/or maintain access

Figure 2: Valid Account Execution

APT15, APT 31, Volt Typhoon, and Storm 0558

APT15 and APT31 are sophisticated Chinese cyber espionage groups known for widespread spear-phishing campaigns and exploitation of public-facing applications to gain initial access, particularly targeting trade, finance, energy, military, and government entities globally according to industry threat intelligence and open-source reporting.[5] Both monitor network traffic and collect sensitive data for military, economic, and diplomatic objectives. Once inside, APT31 obfuscates its activities through front companies[6]. The U.S. sanctioned an APT31-linked firm in March 2024 for targeting CI.[7]

Additionally, a cluster of Volt Typhoon activity in December 2023 and January 2024 **exploited public-facing applications** [T1190] and **external remote services** [T1133] to target U.S. energy and defense sectors, according to industry threat intelligence.[8] Threat actors used public-facing Citrix Netscaler ADC and Ivanti Connect Secure to gain initial access into sensitive systems by leveraging vulnerabilities in the software, to then move deeper into the network, establish backdoors, and monitor activity for espionage or prepositioning purposes.

In June 2023, Microsoft observed PRC-actor Storm-0558 used Azure Active Directory (Azure AD) tokens to access valid U.S. government email accounts. The actors exploited a validation error in Microsoft code to acquire a Microsoft account (MSA) signing key, which they then used to forge the Azure AD tokens needed to access 25 different accounts (including U.S. State Department and Department of Commerce accounts) to gain initial access to the network [T1078].[9,]

IMPACT: In many ways, successful entry is the first cataloged achievement for a malicious actor. With internal access, attackers are privy to private systems and information. The next step of the attack, whether it be code execution, mission disruption, gaining increased privileges, or maintaining unauthorized access for future disruption may not be possible without initial access.

[5] Toulas, B., "Chinese APT15 hackers resurface with new 'Graphican' malware," June 21, 2023, https://www.bleepingcomputer.com/news/security/chinese-apt15-hackers-resurface-with-new-graphican-malware/.

[6] Pomfret, J., & Lun Tian, Y., "APT31: the Chinese hacking group behind global cyberespionage campaign," March 26, 2024, https://www.reuters.com/technology/cybersecurity/apt31-chinese-hacking-group-behind-global-cyberespionage-campaign-2024-03-26/.

[7] U.S. Department of the Treasury, "Treasury Sanctions Six Individuals for Facilitating Financial Transactions for Iranian Malware Operation," March 25, 2024, https://home.treasury.gov/news/press-releases/jy2205.

8 Mandiant Advantage, "Campaign 24.008: Suspected Volt Typhoon-Related Cluster Conducts Citrix Netscaler ADC and Ivanti Connect Secure Exploitation Attempts Against U.S. Energy and Defense Sectors," March 19, 2024, https://advantage.mandiant.com/reports/24-10006049.

[9] Gatlan, S., "Microsoft: Chinese hackers breached US govt Exchange email accounts," July 12, 2023, https://www.bleepingcomputer.com/news/security/microsoft-chinese-hackers-breached-us-govt-exchange-email-accounts/.

Mitigations and Remediations

These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threat TTPs.

- Implement a secure password policy requiring phishing-resistant multifactor authentication (MFA) for remote access, strong passwords, unique credentials, and the separation of user and privileged accounts, effectively revoking unnecessary or inactive accounts. (CPG 2.A-2.X Protect)
- Configure email servers to filter out and block emails with malicious indicators and implement authentication protocols, such as Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) to prevent spoofed or modified emails. (CPG 2.M Email Security)
- Implement a phishing awareness training program that includes guidance on identifying phishing attacks and how personnel should report suspected phishing attempts and verified incidents. (CPG 2.I Basic Cybersecurity Training)
- Establish secure configuration baselines for user systems with macros disabled by default. (CPG 2.N Disable Macros by Default, CPG 2.O Document Device Configurations)
- Maintain up-to-date and fully patched software for all public-facing resources by leveraging a comprehensive asset inventory that tracks installed software version information. (CPG 1.A Asset Inventory, 1.E Mitigating Known Vulnerabilities)
- Log all unsuccessful logins and send to an organization's security team or relevant logging system as an alert to be stored for retroactive analysis. Enforce unsuccessful login attempt policies to disable logins to prevent automated, credential-based attacks. (CPG 2.G Detection of Unsuccessful Login Attempts, CPG 2.T Log Collection).
- Disable unnecessary operating system (OS) applications and network protocols. (CPG 2.W No Exploitable Services on the Internet)
- Maintain a public vulnerability disclosure reporting program so security researchers can provide notice and documentation of identified vulnerabilities on organization assets. (CPG 4.B Vulnerability Disclosure/Reporting)
- Leverage cyber threat intelligence to inform detection mechanisms for relevant cyber threats and associated TTPs. (CPG 3.A Detecting Relevant Threats and TTPs)

EXECUTION

WHAT

During execution, threat actors deploy various tools needed to conduct the attack via executing malicious code. Threat actors can execute malicious code on local or remote systems on the network as an entry method to eventually exfiltrate data. Threat actors leverage malicious code for a variety of reasons, such as establishing backdoors, modifying account privileges, and infecting multiple devices on a network. Threat actors rely on this technique to maintain network access and control.

HOW

The assessments team used **Command-Line Interface (CLI)** [T1059], which is a text-based interface used to interact with computer systems to successfully execute commands. CLI made up **10.3%** of the assessment team's successful execution techniques. Leveraging the CLI allowed the team to install and run new software, including malicious tools. Additionally, the team leveraged **User Execution** [T0863] in **10.1%** of instances, meaning they relied on specific actions by the user to gain execution, such as executing malicious code by opening a malicious document file or link, or enabling Remote Access Software to give direct control of the system to the adversary. Threat actors may use social engineering to direct targets to click on files or links to malicious websites.

Volt Typhoon

Similar to CISA and USCG assessment teams, Volt Typhoon actors rarely use malware for post-compromise execution. Instead, once Volt Typhoon actors gain access to target environments, they use hands-on-keyboard activity via the CLI [T1059] and other native tools and processes on systems [T1218] that were also used by CISA and USCG assessment teams (e.g. Mshta, Control Panel Items, Rundll32, Compiled HTML file).[10] These native tools are known to facilitate Living-Off-The-Land (LOTL), to maintain and expand access to victim networks. CISA and USCG assessment teams focus on limiting damage to the entity, and steer away from using malware and malicious code. Note however, that many threat actors looking to cause damage will execute malicious payloads through other TTPs in this stage.

[10] CISA Alert (AA24-038A): February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

IMPACT

Execution during an attack helps the cyber actor interrupt availability of systems and manipulate data and files. After achieving initial access into the system or network, the threat actor can start to carry out their attack by disrupting daily operations, spreading malware through the network, and preparing to compromise data.

Mitigations and Remediations

- Volt Typhoon often target end-of-life technology that are beyond manufacturer's supported lifecycle. Organizations should consider replacing legacy and outdated technology.
- Maintain up-to-date and fully patched software for all public-facing resources by leveraging a comprehensive asset inventory that tracks installed software version information. (CPG 1.A Asset Inventory, 1.E Mitigating Known Vulnerabilities)
- Prevent lateral movement and privilege escalation through network segmentation and blocking all outbound connections from internet-facing servers. Use demilitarized zones (DMZs) and virtual private networks (VPNs) in network topologies and architectures and configure communication protocols appropriately. (CPG 2.F Network Segmentation).
- Leverage allowlists or other mechanisms to limit installed software and software functionality to the minimum necessary. (CPG 2.Q Hardware and Software Approval Process)
- Collect and store access and security-focused logs for both detection and incident response activities. (CPG 2.T Log Collection)
- Leverage cyber threat intelligence to inform detection mechanisms for relevant cyber threats and associated TTPs. (CPG 3.A Detecting Relevant Threats and TTPs)

PERSISTENCE

WHAT

Persistence requires an attacker to maintain a foothold in a target network for an extended period, sometimes with the ability to survive reboots. Threat actors use persistence techniques, such as changing credentials or system configurations to match their own needs and to maintain their foothold in the system. Persistence in a network is important, providing time for cyber threat actors to identify the data to compromise and collect and quietly disrupt day-to-day operations. Fulfillment of both goals requires prolonged, undetected access to target systems while operating from remote locations.

HOW

To remain persistent on a network, the assessments team used **Valid Accounts** [T0178] in **42%** of instances. After obtaining initial access to domain administrator accounts, valid accounts are also used to bypass access controls placed on various resources across systems within the network. Valid accounts may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access (OWA), and remote desktops or remote management interfaces. The assessments team also used **Hidden Files and Directories** [T1564.001] approximately **15%** of the time to maintain access on the network. Adversaries may set files and directories to be hidden to evade detection mechanisms, such as through antivirus software and security tools that may not scan hidden files by default. They may also use techniques such as file and directory attributes to mark files as hidden, making them less likely to be noticed during manual inspection.

Volt Typhoon and UNC5174

Volt Typhoon primarily relies on valid credentials for persistence [T1078]. By accessing valid accounts and behaving as a valid user would, Volt Typhoon's activity can be very difficult to detect. This focus on operational security has allowed the actor to remain undetected in some target networks for periods lasting up to several years.[11] Mandiant has identified another PRC-affiliated group known as UNC5174, which engages in intrusions for profit. This group sells persistent access via remote services like ScreenConnect and F5 Big-IP, often by furnishing threat actors with valid credentials or remote service application exploits.[12] This approach enables threat actors to maintain access covertly using legitimate management software, thus evading detection.

IMPACT

When threat actors are persistent on a network, they retain the ability to re-infect machines and/or maintain their existing foothold within a network. Persistence on a network allows threat actors to go undetected for months, enabling them to carry out malicious activity or continuously compromise confidential data.

Mitigations and Remediations

- Implement a secure password policy requiring phishing-resistant MFA for remote access, strong passwords, unique credentials, and the separation of user and privileged accounts that effectively revokes unnecessary or inactive accounts. (CPG 2.A–2.H Account Security)
- Audit event logs to detect account manipulation leveraging known threat actor TTPs informed by cyber threat intelligence. (CPG 2.T Log Collection, CPG 2.U Secure Log Storage, CPG 3.A Detecting Relevant Threats and TTPs)

PRIVILEGE ESCALATION

WHAT

Threat actors often gain initial access through a standard user account, which often has limited access to information. To ensure successful exploitation and compromise, threat actors frequently escalate privileges prior to conducting attacks to reach across the network or access the most information possible. To carry out successful operations, threat actors escalate their privileges to domain or administrative level and then explore deeper into networks or access sensitive data. Unaware employees of organizations are often targets of opportunity for threat actors to gain initial access and elevate their level of privilege.

[11] CISA Alert (AA24-038A): February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[12] Lyons, J., "Chinese hackers exploit F5, ConnectWise to seize control of scores of US targets," March 22, 2024, https://www.theregister.com/2024/03/22/china_f5_connectwise_unc5174/.

HOW

The assessments team escalated privileges using **Valid Accounts** [T1078] in **45%** of instances. Use of valid administrator accounts can be achieved via multiple means, such as using hard-coded credentials, using default credentials, or guessing passwords from OS hash dumps. The USCG found that 94.4% of their assessed entities had default passwords in place. Often, the same administrator account obtained during initial access and persistence can be used for privilege escalation. Assessment teams used different methods of Valid Accounts [T1078] depending on whether they were internal to the network or external. Once inside the network, they scan for protocols and find lists of users within the network to access those with higher privileges. Additionally, the team used **Process Injection** [T1631] to evade process-based defenses in **18%** of instances. Process injection is a method of running code in the context of another process that allows access to the memory, or system/network resources.[13]

UNC4992

Threat actors leverage a variety of techniques to escalate privileges [TA0004] within a network. According to Mandiant, UNC4992 is a China-based cyber espionage group that uses social engineering, particularly in open forums, to both lure victims to exploit-hosting infrastructure and to prompt installation of malicious mobile applications. Once in the system, the group is known to use Process Injection [T1055] to execute arbitrary code and escalate privileges on an infected device, posing a threat to communications over both desktop and mobile devices.[14]

[13] MITRE ATT&CK. (2017, March 31). T1055: Process Injection. MITRE ATT&CK. Retrieved from https://attack.mitre.org/techniques/T1055/ -

[14] Mandiant, "Threat Actor Details: Threat Actor [UNC4992]," updated March 14, 2024, https://advantage.mandiant.com/actors/threat-actor--67522f94-8e7e-51f9-b7d5-6a1b0b301970#details.

IMPACT

Successful privilege escalation grants unauthorized privileged access to sensitive data, systems, or processes. Even with internal access, attackers with limited privileges may be restricted from carrying out actions with critically severe results. However, attackers with domain administrator account access, could impair mission-critical functions, potentially leading to the loss of resources. A threat actor could also pivot into Operational Technology (OT) systems or execute more sophisticated attacks that exploit vulnerabilities within the network, such as operating systems and applications that can disrupt critical operations. Escalating into OT systems can bridge the cyber/physical plane.

Mitigations and Remediations

- Prevent privilege escalation by segmenting networks and denying connections from IT to OT assets unless explicitly allowed (CPG 2.F Network Segmentation).
- Secure passwords and sensitive data by not storing passwords and sensitive data in plaintext, with granular access control, and blocking all outbound connections from internet-facing servers. (CPG 2.L Secure Sensitive Data)
- Implement a secure password policy and audit account usage across system and event logs to detect anomalous behavior. (CPG 2.A –2.H Account Security)
- Audit event logs to detect account manipulation that leverages known threat actor TTPs informed by cyber threat intelligence. (CPG 2.T Log Collection, CPG 2.U Secure Log Storage, CPG 3.A Detecting Relevant Threats and TTPs)

DEFENSE EVASION

WHAT

Threat actors use defense evasion techniques [TA0005] to navigate systems and networks undetected for as long as possible. The longer a cyber threat actor goes unnoticed on the system or network, the longer they can carry out operations. Defense evasion techniques include disabling security software or obfuscating data to allow threat actors to navigate throughout the network without the victim noticing. Defense evasion techniques do not require significant resources.

HOW

Threat actors use many different defense evasion techniques, which range from disabling security software to cross-site scripting. The assessments teams also used **Valid Accounts** in **14%** of instances, allowing them to go unnoticed on the network for an extended period. Similar to other steps in the ATT&CK framework, the same accounts accessed previously can be reused for defense evasion. Additionally, the teams used System Binary Proxy Execution: **Mshta** [T1218.005] and Process Injection [T1055] in **7%** of instances to allow malicious code execution. Mshta.exe is a native utility that executes Microsoft HTML Applications files.[15] Threat actors may use Mshta to execute scripts and payloads, bypassing traditional antivirus detection mechanisms. Other native tools were also used for defense evasion, such as Control Panel Items, Hidden Files and Rundll32, Compiled HTML Files, and Signed Binary Proxy Execution [T1218].

[15] MITRE ATT&CK. T1218.005: Signed Binary Proxy Execution. https://attack.mitre.org/techniques/T1218/005/

Volt Typhoon

Volt Typhoon has strong operational security to remain undetected for months or even years at a time. Their actors primarily use LOTL for Defense Evasion [TA0005], which allows them to camouflage their malicious activity with typical system and network behavior, potentially circumventing simplistic endpoint security capabilities.

Volt Typhoon actors also obfuscate their malware. In one confirmed compromise, Volt Typhoon obfuscated a proxy server and a port scanner by compressing the files so a firewall or Intrusion Detection System (IDS) would not detect them [T1027.002].[16] The proxy file applications support encryption, compression, and easy token authentication and, when installed on a legitimate server, connect it to one of Volt Typhoon's malicious servers, according to CISA and agency partner threat analysis.[17]

In addition to LOTL and obfuscation techniques, Volt Typhoon actors have been observed selectively clearing Windows Event Logs [T1070.001], system logs, and other technical artifacts to remove evidence [T1070.009] of their intrusion activity and masquerading file names [T1036.005].

IMPACT

If threat actors remain on networks undetected for extended periods of time, they can disrupt daily operations and impact the organization's mission. As threat actors continue to maintain a foothold in the environment, they access and exfiltrate sensitive data, perform extensive reconnaissance to understand the network and business procedures, and ultimately preposition for disruption, if prompted.

Mitigations and Remediations

- Implement a secure password policy and secure storage of credentials with encryption, prohibiting hard-coded credentials or use of default credentials. (CPG 2.A–2.H Account Security, CPG 2.L Secure Sensitive Data)
- Leverage cyber threat intelligence to inform detection mechanisms of relevant cyber threats and associated TTPs. (CPG 3.A Detecting Relevant Threats and TTPs)

CREDENTIAL ACCESS

WHAT

Threat actors steal credentials to gain access to internal resources, bypass security measures, and confiscate critical data. Use of legitimate credentials gives actors access to systems, conceals their movements and activities, and allows them to create more accounts to help achieve their goals.

[16] CISA Alert (AA24-038A): February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[17] CISA "Malware Analysis Report (AR24-038A)," February 7, 2024, https://www.cisa.gov/news-events/analysis-reports/ar24-038a.

HOW

Threat actors use a variety of techniques, such as keylogging or credential dumping, to steal credentials.

The assessment team leveraged **Credential Dumping** [T1003] in **14%** of instances. Threat actors may attempt to dump credentials to obtain account login and credential information—normally in the form of a hash or a cleartext password—from the OS and software. Threat actors then use dumped credentials to perform lateral movement and access restricted information. Additionally, in **13%** of assessments, the assessments team successfully spoofed an authoritative source for name resolution to force communication with an assessments team-controlled system through Link-Local Multicast Name Resolution and NetBIOS Name Service and Server Message Block (**LLMNR/NBT-NS Poisoning and SMB**).

Volt Typhoon

In a Volt Typhoon campaign that began in 2021 and continued throughout 2023, the actor used compromised Fortinet Fortiguard devices to dump OS [T1003] and domain credentials [T1003.005]. They performed this dumping through the Local Security Authority Subsystem Service (LSASS) process memory space in the form of password hashes.[18] The group has also been observed using Mimikatz and Impacket as credential dumping tools.[19]

IMPACT

If threat actors have access to privileged credentials, it becomes possible to escalate privileges, access sensitive data, and bypass security controls. Credential access could allow threat actors to establish a foothold so that even if the initial intrusion or access was detected, they can maintain access by impersonating a legitimate user.

Mitigations and Remediations

- Implement a secure password policy and audit account usage across system and event logs to detect anomalous behavior. (CPG 2.A–2.H Account Security)
- Restrict remote connections by leveraging host and network security mechanisms and use cyber threat intelligence to inform detections of malicious activity. (CPG 3.A Detecting Relevant Threats and TTPs)

DISCOVERY

WHAT

Discovery is an important phase for the attacker; during discovery, the threat actor attempts to learn about the network, systems, and data. Discovery consists of techniques a threat actor may use to gain knowledge about the system and internal network.

[18] Microsoft Security Team, "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," May 24, 2023, https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.

[19] 19 CISA Alert (AA24-038A): February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

Through these observation techniques, the actor can determine how systems should act and operate. The threat actor also identifies how the environment can assist with their ultimate objective of data exfiltration.

HOW

During discovery, threat actors may try to access a list of useful accounts, such as privileged accounts, on a system or within the network. The assessments team leveraged **Account Discovery** [T1087] in **8%** of instances to identify potentially beneficial accounts for accessing sensitive data. To further identify information, the team used **Password Policy Discovery** [T1201] in **8%** of instances to access detailed information about the password policy used within an enterprise network or cloud environment, which could help the adversary to create a list of common passwords and launch dictionary and/or brute force attacks adhering to the policy. The assessments team tried to uncover information that was available once they entered the network, from file and directory discovery and network sniffing to noting the browser bookmarks, remote software, and security software in place on the systems. Threat actors could do the same if they are able to cover their tracks.

Earth Krahang and Volt Typhoon

According to TrendMicro, PRC-affiliated Earth Krahang scans public-facing servers and uses open-source scanning tools that search for specific folders in networks to target government targets.[20] They also monitor, steal, and read emails to take advantage of trust between government and agencies to refine their targets while searching through filenames and relevant information to discover other exploitation opportunities.[21] Another example-- in its campaign targeting U.S. infrastructure, Volt Typhoon often compromised domains by extracting the Active Directory (AD) database (NTDS.dit) from the domain controller (DC) [T1087]. NTDS.dit is a repository that holds, among other components, usernames and password hashes. Since password hashes are not useful in hash form, researchers suspect Volt Typhoon attempts to crack the passwords offline [T1555 and T1110].[22]

[20] Chen, J., & Lunghi, D., "Earth KRAKHANG: Cyberespionage Campaign Targets ASEAN Nations," March 18, 2024, https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html.

[21] Ibid.

[22] CISA Alert (AA24-038A): February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

IMPACT

During discovery, threat actors gain context regarding a victim's network and gain an understanding of important accounts, the network, and assets, enabling access to critical data. It is important to deploy the proper safeguards to ensure cyber actors cannot easily access critical systems and data, even if they gain access to administrative accounts.

Mitigations and Remediations

- Implement network segmentation to separate resources by sensitivity and/or function, limiting cross-segment communications to those necessary for business functions. (CPG 2.F Network Segmentation)
- Collect and store access and security-focused logs for both detection and incident response activities. (CPG 2.T Log Collection)
- Leverage cyber threat intelligence to inform detection mechanisms for relevant cyber threats and associated TTPs. (CPG 3.A Detecting Relevant Threats and TTPs)

LATERAL MOVEMENT

WHAT

Lateral movement is the process of pivoting from host to host or from one user account to another to reposition, supplement, or spread the active foothold. After obtaining initial access, cyber threat actors conduct these activities, often to move to network locations of specific interest. Threat actors frequently compromise accounts that do not have access to the correct networks or data of interest. To gain access to the correct network or data, threat actors will laterally move from account to account throughout the environment, moving from host to host until they reach the location within the target environment necessary to conduct further attack steps.

HOW

Threat actors such as Volt Typhoon may use their own remote access tools or compromised credentials to laterally move throughout the network and are known to use **Remote Desktop Protocol** (RDP) [T1021.001], **Telnet**, and **SSH**. A number of remote services used by threat actors were also used in assessments [T1021] including RDP and **Windows Admin Shares** [T1021.002]. After obtaining accounts throughout the ATT&CK stages, the assessment team used **Pass the Hash (PtH)** [T1550.003] **(PtH)** attacks in **27%** and **Pass the Ticket** [T1550.003] in **17%** of instances to laterally move through the network. PtH bypasses supplying account passwords by submitting the password hashes to the authentication process. PtH may provide threat actors authenticated access to systems without the need to discover the compromised user account plaintext password. Pass the ticket is a method of authenticating to a system using Kerberos tickets without having access to an account's password.

APT15 and Volt Typhoon

PRC threat actors such as APT15 and Volt Typhoon have been observed predominantly employing RDP with compromised valid administrator credentials, as well as other remote services such as telnet, SSH, and Virtual Networking Computing.[23] With a full, on-premise Microsoft Active Directory identity compromise (see the Credential Access section), the group may be capable of using other methods such as Pass the Hash or Pass the Ticket for lateral movement [T1550].

In one confirmed compromise of a Water and Wastewater Systems Sector entity, “Volt Typhoon actors connected to the network via a VPN with administrator credentials they obtained and opened an RDP session with the same credentials to move laterally.”[24] Over a nine-month period, they moved laterally to several servers, obtained domain credentials from the domain controller, and performed discovery, collection, and exfiltration on the file server.

IMPACT

Many organizations have systems or data deemed critical to achieving their mission on their networks. These systems are typically located in network segments with increased protections, and access can be restricted based on user roles and privilege level. However, a threat actor may be able to access critical systems if allowed to pivot from host to host within a compromised environment. In some instances, this is the stage where threat actors move into OT assets for pre-positioning to conduct physical damage, if intended. Limiting a threat actor’s lateral movement constrains their activity to a confined space, potentially preventing their ability to meet their target objectives.

Mitigations and Remediations

- Enforce phishing-resistant MFA for remote endpoint access and restrict accounts with remote access privileges, prohibiting reuse of passwords across accounts. (CPG 2.H Phishing-Resistant MFA, CPG 2.E Separating User and Privileged Accounts, CPG 2.C Unique Credentials)
- Implement network segmentation to separate resources by sensitivity and/or function, limiting cross-segment communications to those necessary for business functions. (CPG 2.F Network Segmentation)
- Manage access permissions and authorizations with the principle of least privilege, granting the minimum access to a system’s resources unless authorized.
- Audit system and event logs to detect abnormal account activity, focusing detections based on insights from cyber threat intelligence. (CPG 2.T Log Collection, CPG 2.U Secure Log Storage, CPG 3.A Detecting Relevant Threats and TTPs)

[23] Mandiant. Threat Actor Details: Threat Actor [APT 15]. https://advantage.mandiant.com/actors/threat-actork

[24] CISA Alert (AA24-038A): February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

COLLECTION

WHAT

After threat actors establish a presence within an organization's network, they collect sensitive internal data for a variety of reasons, which can include gaining competitive advantage. Many threat actors gather information using various techniques, such as capturing screenshots and keyboard inputs. Data collection assists intelligence or surveillance efforts for future operations or can help threat actors gain financial profit. Ultimately, data collection is key to successful malicious operations.

HOW

Threat actors carry out collection in a variety of ways. The assessments team revealed that **Data from Network Shared Drives** constituted **42%** of successful data access attempts. Organizations often use network shares to segment data for role-based access, such as admin shares. Threat actors leverage weaknesses, such as misconfigured permissions, within network shares to collect data. Additionally, the team obtained sensitive **Data from Local Systems** in **29%** of instances. The team could locate local file systems and databases, which granted access to sensitive information.

Earth Krahang

According to TrendMicro, PRC threat actor Earth Krahang has used collection in an ongoing campaign that continued throughout 2023 targeting entities that included U.S. government agencies. Malware and tools the actor deploys include CobaltStrike, RESHELL, and XDealer, which provide **Automated Collection** [T1119] and **Email Collection** [T1114] capabilities, as well as screenshots, keystrokes, and clipboard data.[25]

IMPACT

Allowing threat actors to locate and collect sensitive data negates the intended function of network security, communications security, operational security, and physical security efforts.

Mitigations and Remediations

- Monitor access logs and network communication logs to detect abnormal access to and transfer of data. (CPG 2.T Log Collection, CPG 2.U Secure Log Storage, CPG 3.A Detecting Relevant Threats and TTPs)
- Ensure encryption standards for data transfers and web applications are up to standard and data is encrypted through all phases, including the hard drive for storage, browser, and transfer (CPG 2.K Strong and Agile Encryption)
- Consider establishing classification program for sensitive data.

COMMAND AND CONTROL (C2)

WHAT

An ongoing attack requires a threat actor to maintain persistence in a target network for continued access to the environment.

[25] Chen, J., & Lunghi, D., "Earth KRAKHANG: Cyberespionage Campaign Targets ASEAN Nations," March 18, 2024, https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html.

By establishing a hidden communications channel between remote servers and compromised systems within the target network, actors conduct internal activity while avoiding detection. Depending on the overall intent of a malicious campaign, attacks may span the course of several weeks or months. Threat actors operating at remote locations need prolonged, undetected access to targeted systems to identify and collect sensitive data and to quietly disrupt day-to-day operations.

HOW

Threat actors use C2 techniques to communicate with compromised systems. The assessments team deployed C2 channels using **Commonly Used Ports** [T1571] in **19%** of their successful attempts, which can include port 80 (HTTP), 443 (HTTPS), 3389 (Remote Desktop Protocol) and others. Techniques such as **Data Obfuscation** [T1001] made up **12%** of successful RVA attacks, where a threat actor obfuscates C2 traffic to make it more difficult to discover, thus hiding commands.

ChamelGang

In a campaign that continued into 2023, PRC-affiliated threat actor ChamelGang, used DNS-over-HTTPS (DoH) [T0885] to establish C2 [TA0011] on Linux devices. DoH uses Port 443, the commonly used default port for HTTPS, to encrypt DNS traffic. This not only secures the traffic from snooping, but it also allows the traffic to blend in with legitimate HTTPS traffic and challenges efforts to analyze DNS traffic.[26,27] The reporting did not mention entities specifically targeted in this campaign, but ChamelGang has historically targeted U.S. entities.

IMPACT

The use of undetected control channels to conduct operations remotely allows threat actors the anonymity and stealth needed to operate on a victim network uninterrupted until they achieve their mission objectives.

Mitigations and Remediations

- Implement detections informed by cyber threat intelligence against centralized logging to alert on potentially malicious activity. (CPG 2.T Log Collection, CPG 2.U Secure Log Storage, CPG 3.A Detecting Relevant Threats and TTPs)

EXFILTRATION

WHAT

Threat actors use a variety of exfiltration techniques to steal data from victim networks; threat actors may target sensitive information, such as blueprints, security requirements documents, or vulnerability information, on a compromised system or network enclave. Many actors conduct attacks to gain access to financial information, sensitive security data, or personally identifiable information (PII).

[26] Mayer, D., "ChamelGang and ChamelDoh: A DNS over HTTPS Implant," July 3, 2023, https://stairwell.com/resources/chamelgang-and-chameldoh-a-dns-over-https-implant/

[27] Toulas, B., "Chinese hackers use DNS-over-HTTPS for Linux malware communication," June 14, 2023, https://www.bleepingcomputer.com/news/security/chinese-hackers-use-dns-over-https-for-linux-malware-communication/.

By stealing this data, actors may be able to analyze organizational information from the safety of their remote location. Even if their activity is detected by the compromised organization, the stolen data is still available to the threat actors for later use.

HOW

Threat actors use a variety of techniques to exfiltrate data. The assessments team successfully **Exfiltrated Data Over the C2 Channel** [T1041] in **41%** of instances. Using the C2 channel established for remote access allowed the assessments team to download information without establishing additional pathways or potentially alerting network defenders. Additionally, the team **Exfiltrated Over Alternative Protocol** [T1048] in **14%** of instances to successfully exfiltrate data over a network outside of the existing C2 server. Threat actors will use similar techniques, while also exploiting vulnerabilities to meet their final objectives. Because assessments do not ultimately want to exfiltrate vast amounts of data, the tactics in this stage can be more tailored by real world threat actors.

UNC4841 and APT41

Between October 2022 and May 2023, PRC threat actor UNC4841 performed multiple exfiltration operations on Barracuda Email Security Gateway (ESG) via Seaspy, a backdoor that monitors traffic from a threat actor's C2 server [T1646], according to CISA and open-source reporting.[28] Over 200,000 entities worldwide were affected, to include those in the U.S. Food and Agriculture and the Transportation Systems Sectors. The actors exploited remote command injection flaw CVE-2023-2868 to establish a series of connections and payloads to ultimately load Seaspy to passively act as a packet filter on the ESG.[29,30]

In another example, "APT41 leveraged Cloudflare Workers to deploy serverless code accessible through the Cloudflare Content Delivery Network (CDN) which helps proxy C2 traffic to APT41 operated infrastructure… APT41 leveraged [this] technique for further data exfiltration by hex encoding PII data and prepending the results as subdomains of the attacker-controlled domain. The resulting DNS lookups triggered by the ping commands would be recorded in the activity logs and available to APT41," according to Mandiant.[31]

[28] Toulas, B.,. (2023, June 15). Barracuda ESG zero-day attacks linked to suspected Chinese hackers. *BleepingComputer.* https://www.bleepingcomputer.com/news/security/barracuda-esg-zero-day-attacks-linked-to-suspected-chinese-hackers/

[29] CISA. "CISA Releases Malware Analysis Reports on Barracuda Backdoors," September 7, 2023, https://www.cisa.gov/news-events/alerts/2023/07/28/cisa-releases-malware-analysis-reports-barracuda-backdoors.

[30] Gatlan, S., "CISA warns govt agencies of recently patched Barracuda zero-day," May 27, 2023, https://www.bleepingcomputer.com/news/security/cisa-warns-govt-agencies-of-recently-patched-barracuda-zero-day/.

[31] Rufus Brown et al., "Does This Look Infected? A Summary of APT41 Targeting US State Governments," Mandiant, March 23, 2023, https://www.mandiant.com/resources/blog/apt41-us-state-governments.

IMPACT Threat actors try to manipulate, interrupt, steal, or destroy victim information or assets. When a malicious actor successfully exfiltrates data, they impact the victim's reputation, release sensitive data impacting other users, or disrupt day-to-day operations.

Mitigations and Remediations

- Implement detections informed by cyber threat intelligence against centralized logging to alert on potentially malicious activity. (CPG 2.T Log Collection, CPG 2.U Secure Log Storage, CPG 3.A Detecting Relevant Threats and TTPs)
- Separately from the source system and no less than once per year, back up systems necessary for operations. (CPG 2.R System Backups)

CONCLUSION

After conducting trend analysis on the networks and network defenses of the entities in the 143 RVAs, CISA and the USCG made high-level observations that would improve the ability of CI organizations to secure and protect their networks. Throughout the assessment lifecycle, **Valid Accounts** was the most prominent technique used across multiple tactics. Although CISA and the USCG teams do not directly emulate an adversary, they locate any conditions present in the environment, or use opportunistic techniques. In previous years, assessors primarily used **Valid Accounts** to gain initial access into the network. However, in FY23, they found opportunities to use **Valid Accounts** to move laterally through the network, evade defenses, and escalate privileges, although in many cases, the same accounts can be used in several stages of the ATT&CK framework. Therefore, a threat actor can do a lot with a small number of credentials accessed early on, especially when Microsoft Active Directory database is extracted using a domain account.

To guard against the successful abuse of **Valid Accounts**, CI entities should:

- Implement strong password policies and phishing-resistant MFA.
- Implement Identity Access Management solution and granular access control to lock down privileged accounts, protect user credentials, and facilitate assigning users to groups with specific permissions.
- Monitor access logs and network communication logs to detect abnormal access.
- Swiftly identify and respond to detected abnormalities to reduce potential damage.

To deter a cyber threat actor's ability to compromise systems or networks, CI entities should implement mitigations-centered intrusion prevention, such as:

- Deploying a centralized cyber threat intelligence platform to monitor and log critical data and using the platform to detect and remediate abnormal behavior in a timely manner.
- Implementing a secure network security architecture with multiple layers of protections—using next-generation firewalls, granular access controls, network segmentation, SIEM/SOAR, robust encryption, and secure communication.
- Implementing enhanced protection mechanisms alongside strong credential policies

CISA encourages system owners and administrators to share this guidance with leadership and apply relevant changes tailored to their specific environments. Analysis of this nature can effectively prioritize the identification and mitigation of high-level vulnerabilities across multiple sectors and entities.

REFERENCES

Brown, Rufus, Van Ta, Douglas Bienstock, Geoff Ackerman, and John Wolfram. “Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments.” Mandiant (blog), March 8, 2022. https://www.mandiant.com/resources/blog/apt41-us-state-governments.

Chen, J., & Lunghi, D. (2024, March 18). Earth KRAKHANG: Cyberespionage Campaign Targets ASEAN Nations. *Trend Micro.* Retrieved from https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html

Cybersecurity and Infrastructure Security Agency (CISA). (2023, September 7). CISA Releases Malware Analysis Reports on Barracuda Backdoors. *CISA.* Retrieved from https://www.cisa.gov/news-events/alerts/2023/07/28/cisa-releases-malware-analysis-reports-barracuda-backdoors

Cybersecurity and Infrastructure Security Agency (CISA). (2024, February 7). Alert (AA24-038A): PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. CI. *CISA.* Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

Gatlan, S. (2023, May 27). CISA warns govt agencies of recently patched Barracuda zero-day. *BleepingComputer.* Retrieved from https://www.bleepingcomputer.com/news/security/cisa-warns-govt-agencies-of-recently-patched-barracuda-zero-day/

Lyons, J. (2024, March 22). Chinese hackers exploit F5, ConnectWise to seize control of scores of US targets. *The Register.* Retrieved from https://www.theregister.com/2024/03/22/china_f5_connectwise_unc5174/

Mandiant. (updated 2024, March 14). Threat Actor Details: Threat Actor [UNC4992]. *Mandiant Advantage.* Retrieved from https://advantage.mandiant.com/actors/threat-actor--67522f94-8e7e-51f9-b7d5-6a1b0b301970#details

Mandiant. (2024, March 21). Initial Access Brokers Exploit F5 & ScreenConnect. *Mandiant (blog).* Retrieved from https://www.mandiant.com/resources/blog/initial-access-brokers-exploit-f5-screenconnect

Microsoft Security Team. (2023, May 24). Volt Typhoon targets US critical infrastructure with living-off-the-land techniques. *Microsoft Security Blog.* Retrieved from https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

MITRE ATT&CK. (2017, March 31). T1055: Process Injection. *MITRE ATT&CK.* Retrieved from https://attack.mitre.org/techniques/T1055/#:~:text=Process%20injection%20is%20a%20method%20of%20executing%20arbitrary,process%27s%20memory%2C%20system%2Fnetwork%20resources%2C%20and%20possibly%20elevated%20privileges.

MITRE ATT&CK. (2020, January 23). T1218.005: Signed Binary Proxy Execution. *MITRE ATT&CK.* Retrieved from https://attack.mitre.org/techniques/T1218/005/

Phishing Infographic. (n.d.). *Cybersecurity and Infrastructure Security Agency (CISA).* Retrieved from https://www.cisa.gov/sites/default/files/publications/phishing-infographic-508c.pdf

Pomfret, J., & Lun Tian, Y. (2024, March 26). APT31: the Chinese hacking group behind global cyberespionage campaign. *Reuters.* Retrieved from https://www.reuters.com/technology/cybersecurity/apt31-chinese-hacking-group-behind-global-cyberespionage-campaign-2024-03-26/

Ragi, M., Aprahamian, A., Kelly, D., Potaczeck, M., Siedlarz, M., & Larsen, A. (2024, March 21). Initial Access Brokers Exploit F5 & ScreenConnect. *Mandiant (blog).* Retrieved from https://www.mandiant.com/resources/blog/initial-access-brokers-exploit-f5-screenconnect

Sjouwerman, S. (2022, September 8). Initial Access Brokers: The New Face of Organized Cybercrime. *Security Magazine.* Retrieved from https://www.securitymagazine.com/articles/98405-initial-access-brokers-the-new-face-of-organized-cybercrime

Toulas, B. (2023, June 14). Chinese hackers use DNS-over-HTTPS for Linux malware communication. *BleepingComputer.* Retrieved from https://www.bleepingcomputer.com/news/security/chinese-hackers-use-dns-over-https-for-linux-malware-communication/

Toulas, B. (2023, June 21). Chinese APT15 hackers resurface with new 'Graphican' malware. *BleepingComputer.* Retrieved from https://www.bleepingcomputer.com/news/security/chinese-apt15-hackers-resurface-with-new-graphican-malware/

U.S. Department of the Treasury. (2024, March 25). Treasury Sanctions Six Individuals for Facilitating Financial Transactions for Iranian Malware Operation. *U.S. Department of the Treasury Press Releases.* Retrieved from https://home.treasury.gov/news/press-releases/jy2205