TLP: CLEAR

CISA Analysis: Fiscal Year 2022 Risk and Vulnerability Assessments

Publication: June 2023

TLP: CLEAR

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 operators; and select state, local, tribal, and territorial (SLTT) stakeholders. Concurrently, the United States Coast Guard (USCG) conducts RVAs on maritime critical infrastructure operated by SLTT and private-sector organizations.

The RVA is intended to assess the entity's network capabilities and network defenses against potential threats. In Fiscal Year 2022 (FY22), CISA and USCG conducted **121** RVAs across multiple critical infrastructure sectors.[1] Each RVA maps the results to the MITRE ATT&CK® framework, which includes 14 tactics that cyber threat actors use to obtain and maintain unauthorized access to a network or system. The 121 RVAs map to 11 of the 14 tactics. The goal of the RVA analysis is to develop effective strategies that positively impact the security posture of FCEB, critical infrastructure, maritime, and SLTT stakeholders.

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

The FY22 reports provided these general observations:

- Threat actors completed their most successful attacks via common methods, such as phishing and using default credentials.
- Threat actors used varied and constantly changing tools and techniques to successfully conduct common attacks.
- Many organizations across varying critical infrastructure sectors exhibited the same vulnerabilities.

ATTACK PATH ANALYSIS

This report analyzes a sample attack path cyber threat actors could leverage to compromise an organization using weaknesses identified in the FY22 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 used—and not all attack paths follow this model—a skilled threat actor could follow this path to successfully exploit a target. The sample attack path highlights the more successful attack strategies used during RVAs and the impacts these strategies have had on target networks.

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

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 access 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.

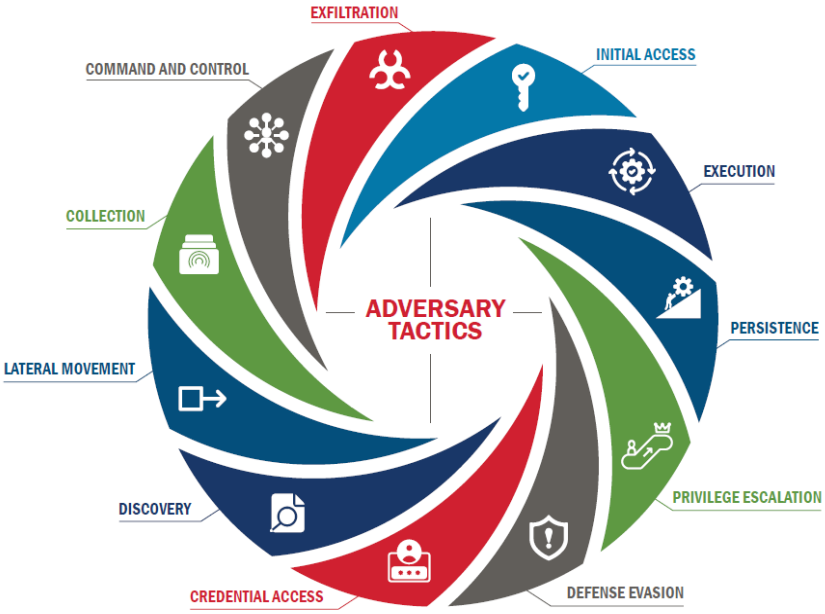

Figure 1: Adversary Tactics

Real-World Attack Paths: APT41

To provide additional context to the sample attack path, this analysis examines the ransomware group APT41, known as “Double Dragon,” to highlight real-world implications of the vulnerabilities successfully exploited through the assessments.

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 the first step in a successful attack. Threat actors could use techniques—e.g., targeted spearphishing or exploiting critical vulnerabilities and weaknesses on public-facing web servers—to gain an initial foothold within a network. If threat actors establish initial access, then they could execute other techniques, such as privilege escalation, to ultimately steal information. Preventing initial access should be a main goal in protecting network assets and data.

HOW

Threat actors use a variety of attack paths, e.g., gaining access to valid accounts, spearphishing, or leveraging insecure ports or protocols, to compromise a victim's network. RVA analyses revealed that **Valid Accounts** were the most common successful attack technique, responsible for **54%** of successful attempts. Valid accounts can be former employee accounts that have not been removed from the active directory or default administrator accounts. When organizations do not change default passwords, threat actors can compromise a valid administrator account. 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.

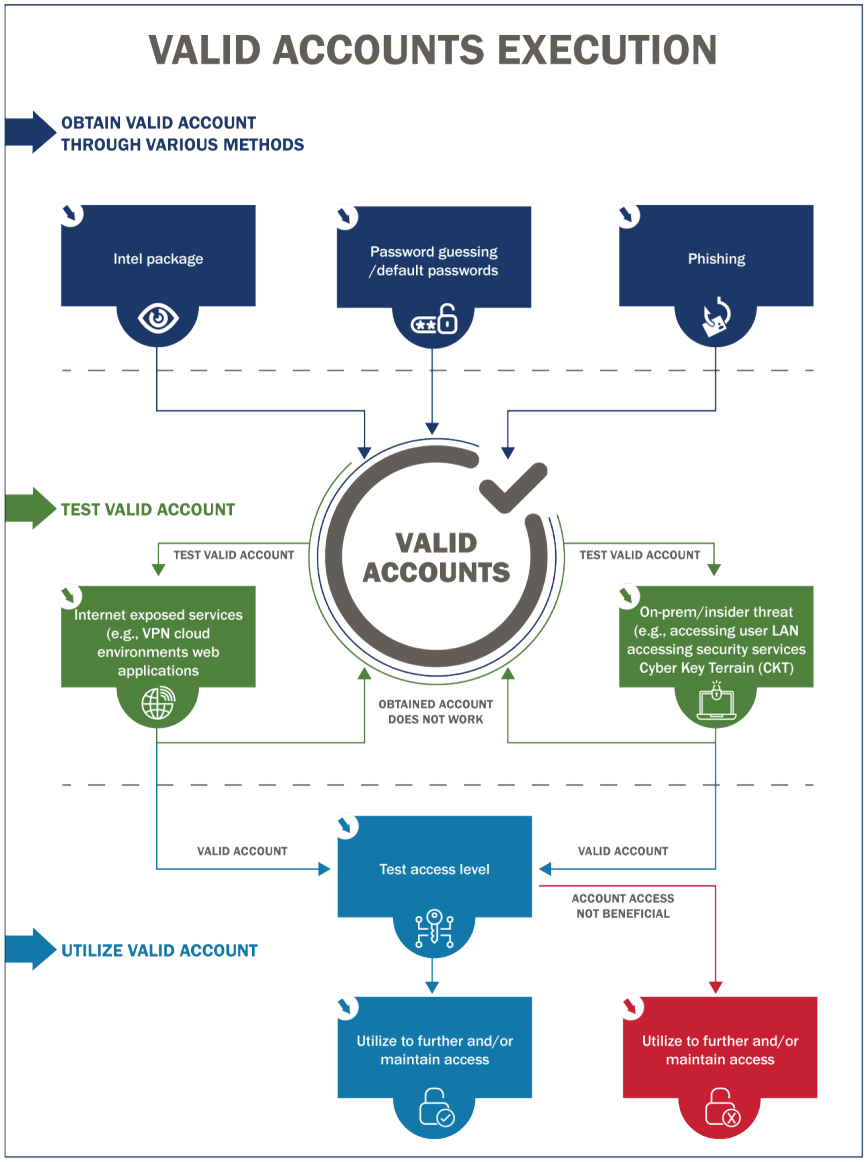

Figure 2: Valid Account Execution

The second most common successful attack technique used **spearphishing links**. Spearphishing 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.[2] The spearphishing link is the delivery of targeted emails with malicious links designed to give the cyber threat actor an entryway into the recipient's network or system. RVA analyses revealed that **Spearphishing Links** were successful **33%** of the time. Successful spearphishing requires an attacker's malicious email to pass through network border protections and deliver malware to execute on the local host. Host-level protection stops spearphishing attempts as they pass through network perimeter protection. At the network border level, CISA observed 13% of spearphishing attempts blocked. At the host or endpoint level, CISA observed 78% of links or attachments blocked, preventing the execution of a malicious activity. 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.

APT41

Ransomware groups like APT41 establish **initial access** by taking advantage of publicly disclosed vulnerabilities to step into the targeted network. APT41 leveraged a critical remote code execution (RCE) vulnerability in the commonly used logging framework Log4J, CVE-2021-44228.[3,4] According to Mandiant, "Within hours of the advisory, APT41 began exploiting the vulnerability to later compromise at least two U.S. state governments and more traditional targets in the insurance and telecommunications industries."[5]

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, or gaining increased privileges, may not be possible without initial access.

---

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

[3] "CVE-2021-4428," National Vulnerability Database (NVD), National Institute of Standards and Technology (NIST), last modified April 3, 2023, https://nvd.nist.gov/vuln/detail/CVE-2021-44228.

[4] Page, Carly. "China-backed APT41 compromised 'at least' six US state governments." Techcrunch+ (blog), March 8, 2022. https://techcrunch.com/2022/03/08/apt41-state-governments/.

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

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 threats, tactics, techniques, and procedures (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)
- 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 the network or on local or remote systems 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 **PowerShell,** which is a task automation and configuration management program from Microsoft consisting of a command-line shell and the associated scripting language. **PowerShell** made up **14%** of the assessment team's successful execution techniques. Additionally, the team leveraged **Command-Line Interface** to successfully interact with systems and execute commands in **12%** of instances. Leveraging the command-line interface allowed the team to install and run new software, including malicious tools. Threat actors download and execute PowerShell scripts to run commands and payloads to further compromise systems and networks.

APT41

Similarly, APT41 relies on executing malicious code within a network. According to Mandiant: "APT41 has primarily used malicious ViewState to trigger code execution against targeted web applications. Within the ASP.NET framework, ViewState is a method for storing the application's page and control values in HTTP requests to and from the server. The ViewState is sent to the server with each HTTP request as a Base64 encoded string in a hidden form field. The web server decodes and applies additional transformations to the string, which allows it to be unpacked into data structures the server can use. This process is known as deserialization."[6]

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

- 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)

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

PERSISTENCE

WHAT

Persistence requires an attacker to maintain a foothold in a target network for an extended period, for example, 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** in **56%** of instances. Valid accounts can be 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 virtual private networks (VPN), Outlook Web Access (OWA), and remote desktops. The assessments team also used **Account Manipulation** approximately **8.7%** of the time to maintain access on the network. During account manipulation, threat actors can modify credentials, permission groups, or network access to subvert security policies.

APT41

According to Mandiant, to maintain persistent execution of DEADEYE, "APT41 has leveraged the computer code to modify existing scheduled tasks that run under the context of SYSTEM." APT41 uses living-off-the-land binaries (lolbin), which are native to the operating system (OS). APT41 also leveraged the following Windows scheduled tasks for persistence of DEADEYE droppers in U.S. state government intrusions:

- \Microsoft\Windows\PLA\Server Manager Performance Monitor
- \Microsoft\Windows\Ras\ManagerMobility
- \Microsoft\Windows\WDI\SrvSetupResults
- \Microsoft\Windows\WDI\USOShared[7]

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 can allow threat actors to go undetected for months, enabling them to carry out malicious activity or continuously compromise confidential data.

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

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 and 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 can 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 carry out successful operations, threat actors escalate privileges to explore networks or access sensitive data. Many methods used to gain initial access target employees of an organization. Victims can be either unaware users or targets of opportunity. Since threat actors target any victim, attackers often begin internal activities with basic user access.

HOW

The assessments team escalated privileges using **Valid Accounts** in **42%** 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. Additionally, the team used **Process Injection** to evade process-based defenses in **19%** of instances**.**

APT41

Threat actors leverage a variety of techniques to escalate privileges within a network. APT41 performed extensive reconnaissance and credential harvesting to escalate privileges. According to Mandiant, “A common tactic seen is the deployment of a ConfuserEx obfuscated BADPOTATO binary to abuse named pipe impersonation for local NT AUTHORITY\SYSTEM privilege escalation. Once APT41 escalated to NT AUTHORITY\SYSTEM privileges, they copied the local SAM and SYSTEM registry hives to a staging directory for credential harvesting and exfiltration. APT41 has additionally used Mimikatz to execute the lsadump::sam command on the dumped registry hives to obtain locally stored credentials and NTLM hashes.”[8]

[8] https://www.mandiant.com/resources/blog/apt41-us-state-governments

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 equipment or resources.

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)
- 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 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 can 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 different defense evasion techniques, which range from disabling security software to cross-site scripting. The assessments team used **Valid Accounts** in **17%** of instances, allowing them to go unnoticed on the network for an extended period. Additionally, the team used **Process Injection** in **8%** of instances to allow malicious code execution. After injecting malicious code into a legitimate process, the threat actor can access legitimate processes' resources, such as process memory, system/network resources, and elevated privileges.

APT41

APT41 leverages a unique defense evasion technique by deploying a Cobalt Strike beacon involving obfuscation of the payload through host software. As noted by Bleeping Computer, “According to the Group-IB report, the cyber threat actors encode the payload in base64 and break it into a large number of smaller pieces consisting of 775 characters, which are then echoed to a text file named dns.txt…”[9]

[9] Bill Toulas, “Winnti hackers split Cobalt Strike into 154 pieces to avoid detection,” *Bleeping Computer,* August 18, 2022, https://www.bleepingcomputer.com/news/security/winnti-hackers-split-cobalt-strike-into-154-pieces-to-evade-detection/.

IMPACT If threat actors remain on networks undetected for extended periods of time, they can disrupt daily operations and impact the organizations mission. As threat actors continue to maintain a foothold in the environment, they can access and exfiltrate sensitive data.

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 steal critical data. Use of legitimate credentials can give actors access to systems, conceal their movements and activities, and allow them to create more accounts to help achieve their goals.

HOW Threat actors use a variety of techniques, such as keylogging or credential dumping, to steal credentials. In **17%** 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**). Additionally, the team leveraged **Credential Dumping** in **17%** 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 can then use dumped credentials to perform lateral movement and access restricted information.

APT41

According to Group-IB, "APT41 campaigns most often involved computer code, such as Ntdsutil. The attackers use the tool to obtain a copy of the ntds.dit file, which is a database that stores Active Directory data, including information about user objects, groups, and group membership. The database also includes the password hashes for all the users of the domain."[10] By accessing the ntds.dit file, APT41 can obtain credential access to a variety of systems and networks.

[10] "APT41 World Tour 2021 on a tight schedule," Group IB, August 18, 2022, https://www.group-ib.com/blog/apt41-world-tour-2021/.

IMPACT If threat actors have access to privileged credentials, it becomes possible to escalate privileges, access sensitive data, and bypass security controls.

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. Through these observation techniques, the actor can determine how systems should act and operate. The threat actor can also identify 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** in **10%** of instances to identify potentially beneficial accounts for accessing sensitive data. To further identify information, the team used **Network Share Discovery** in **10%** of instances to access folders and drives of interest for collection.

APT41

According to Group-IB, APT41 uses the passive scanning tool fofa.su (Peoples Republic of China equivalent of shodan.io) that "scans the internet and collects information regarding open ports and services running on them, which enables attackers to determine their targets and conduct attacks more effectively."[11]

[11] "APT41 World Tour 2021 on a tight schedule," Group IB, August 18, 2022, https://www.group-ib.com/blog/apt41-world-tour-2021/.

IMPACT During discovery, threat actors gain context regarding a victim's network and can 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.

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 may use their own remote access tools or compromised credentials to laterally move throughout the network. The assessments team used **Pass the Hash (PtH)** attacks in **27%** of instances to laterally move through the network. This technique 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. The team also used **Remote Desktop Protocol (RDP)** in **17%** of instances to expand their footprint within the compromised network by remotely accessing and controlling neighboring hosts from previously exploited systems.

APT41

APT41 uses multiple methods to perform lateral movement in an environment, including:

- RDP sessions.
- Using stolen credentials
- Adding accounts to user and admin groups.
- Using password brute-forcing utilities

The group also uses a compromised account to create scheduled tasks on systems or modify legitimate Windows services to install backdoors for continued access and communication

IMPACT Many organizations house systems or data deemed critical to achieving overall mission success 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. 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)
- 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)

COLLECTION

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

HOW Threat actors can carry out collection a variety of ways. The assessments team revealed that **Data from Network Shared Drives** constituted **33%** of successful data access attempts. Organizations often use network shares to segment data for role-based access, such as admin shares. Threat actors can 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.

APT41

Threat actors, such as APT41, rely on collecting data from local systems. APT41 has uploaded files and data from a compromised host.[12]

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)

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. By establishing a hidden communications channel between remote servers and compromised systems within the target network, actors can 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** in **26%** of their successful attempts. Techniques such as **data obfuscation** made up **12%** of successful RVA attacks.

APT41

According to Duo Security, “APT41 leveraged a new malware family that researchers called DustPan, an in-memory dropper that was used to drop a Cobalt Strike beacon backdoor. And after exploiting the Log4j flaw, APT41 deployed a new variant of the KeyPlug backdoor on Linux servers of multiple victims. KeyLog is a modular backdoor that supports multiple network protocols for C2, including HTTP, TCP [Transmission Control Protocol], KCP [KERN Communications Protocol] over UDP [User Datagram Protocol], and WSS [WebSocket Secure].”[13]

[12] Rufus Brown et al., “Does This Look Infected? A Summary of APT41 Targeting US State Governments,” Mandiant, last modified March 23, 2023, https://www.mandiant.com/resources/blog/apt41-us-state-governments.
[13] Lindsey O’Donnell-Welch, “APT41 Compromised Six U.S. State Government Networks,” *Decipher,* March 8, 2022, https://duo.com/decipher/apt41-compromised-six-state-government-networks.

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 enclave. Many actors conduct attacks to gain access to financial information, sensitive security data, or personally identifiable information (PII). 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** in **71%** 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 could **Encrypt Data** in **7%** of instances to successfully exfiltrate data.

APT41

According to Mandiant, "APT41 leveraged Cloudflare Workers to deploy serverless code accessible through the Cloudflare 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."[14]

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

IMPACT Threat actors may try to manipulate, interrupt, steal, or destroy victim information or assets. When a malicious actor successfully exfiltrates data, they can 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 121 RVAs, CISA and USCG made high-level observations that would improve the ability of critical infrastructure organizations to secure and protect their networks.

Throughout the assessment lifecycle, **Valid Accounts** was the most prominent technique used across multiple tactics. In previous years, cyber threat actors primarily used **Valid Accounts** to gain initial access into the network. However, in FY22, cyber threat actors used **Valid Accounts** to move laterally through the network and escalate privileges. To guard against the successful **Valid Accounts** technique, critical infrastructure entities must implement strong password policies, such as phishing-resistant MFA, and monitor access logs and network communication logs to detect abnormal access. Swift identification of abnormalities can reduce damage caused by a cyber intrusion.

To deter a cyber threat actors' ability to compromise a system or network, critical infrastructure entities should implement mitigations-centered intrusion prevention. Critical infrastructure entities should consider implementing enhanced protection mechanisms alongside phishing-resistant MFA and strong password policies. Enhanced protection mechanisms, such as a centralized cyber threat intelligence platform can monitor and log critical data to detect—and, if necessary, remediate—abnormal behavior in a timely manner.

CISA encourages system owners and administrators to share this guidance to their leadership and apply changes relevant to the nuances of their specific environments. CISA concludes that analysis of this nature may 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.

Cybersecurity and Infrastructure Security Agency (CISA). “Cross-Sector Cybersecurity Performance Goals 2022.” CISA, October 2022. https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf.

MITRE Corporation. “*MITRE ATT&CK.”* Last modified May 9, 2023. https://attack.mitre.org.

MITRE Corporation. “APT41.” Last modified March 23, 2023. https://attack.mitre.org/groups/G0096/.

O’Donnell-Welch, Lindsey. “APT41 Compromised Six U.S. State Government Networks.” *Decipher,* March 8, 2022. https://duo.com/decipher/apt41-compromised-six-state-government-networks.

Page, Carly. “China-backed APT41 compromised ‘at least’ six US state governments.” Techcrunch+ (blog), March 8, 2022. https://techcrunch.com/2022/03/08/apt41-state-governments/.

Rostovtsev, Nikita. “APT41 World Tour 2021 on a tight schedule.” Group-IB (blog), August 18, 2022. https://blog.group-ib.com/apt41-world-tour-2021.

Toulas, Bill. “Winnti hackers split Cobalt Strike into 154 pieces to evade detection.” *Bleeping Computer,* August 18, 2022. https://www.bleepingcomputer.com/news/security/winnti-hackers-split-cobalt-strike-into-154-pieces-to-evade-detection/.