TLP:WHITE

CISA Analysis: FY2021 Risk and Vulnerability Assessments

Publication: May 2022

TLP:WHITE

BACKGROUND

Each year, the Cybersecurity and Infrastructure Security Agency (CISA) conducts Risk and Vulnerability Assessments (RVA) of Federal Civilian Executive Branch (FCEB), Critical Infrastructure (CI), and State, Local, Tribal, and Territorial (SLTT) stakeholders. Each RVA is intended to assess the entity's network capabilities and network defenses against potential threats. In Fiscal Year 21 (FY21), CISA conducted 112 RVA assessments of multiple stakeholders across various sectors. As part of each RVA, the results are mapped to the MITRE ATT&CK® framework. The goal of RVA analysis is to develop effective strategies that positively impact the security posture of the FCEB, CI, and SLTT stakeholders.

During each RVA, CISA collects data through onsite assessments and combines it with national threat and vulnerability information to provide organizations with actionable remediation recommendations, prioritized by risk. CISA designed RVAs to identify vulnerabilities that adversaries could exploit to compromise network security controls. RVAs may incorporate the following methodologies:

- Scenario-based network penetration testing
- Web application testing
- Social engineering testing
- Wireless testing
- Configuration reviews of servers and databases
- Detection and response capability evaluation

After completing an RVA, CISA provides the assessed entity with a final report that includes business executive recommendations, specific findings, potential mitigations, and technical attack path details.

PROCESS

CISA's RVA teams leverage the MITRE ATT&CK[1] Framework. The intent of the framework is to build a community-driven knowledge base, comprised of the known tactics, techniques, and procedures (TTPs) of threat actors. The goal of this knowledge base is to aid in the development of threat models and to facilitate vulnerability mitigation efforts. The framework includes 14 tactics that cyber adversaries use to obtain and maintain unauthorized access to a network or system.

Based on the ATT&CK methods used by the CISA Assessment teams and the varying success rates of each, CISA developed a sample attack path. As a skilled threat actor may successfully step through a similar attack path, eventually achieving successful exploitation of their target, CISA structures its assessments to help participating entities evaluate their exposure to such threats and compensate for any weaknesses discovered.

[1] https://us-cert.cisa.gov/best-practices-mitre-attckr-mapping

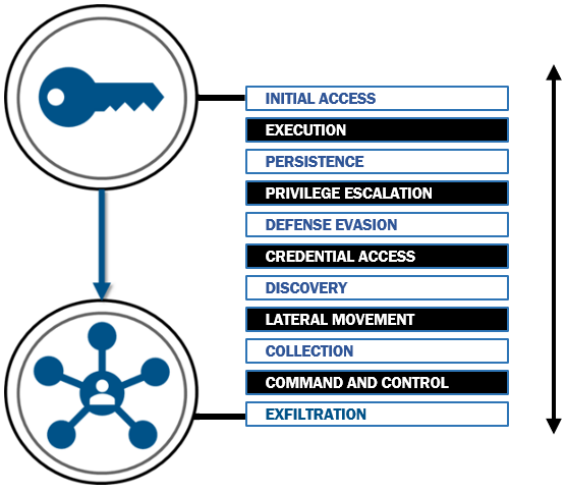
INTRODUCTION

This report analyzes a sample attack path that a cyber threat actor could take to compromise an organization, using weaknesses identified in FY21 RVAs. The path comprises eleven successive tactics or steps: *Initial Access*, *Execution*, *Persistence*, *Privilege Escalation*, *Defense Evasion*, *Credential Access*, *Discovery*, *Lateral Movement*, *Collection*, *Command and Control*, and *Exfiltration*. In addition to this analysis, the report includes the following observations:

- Most successful attacks were achieved through methods commonly used by threat actors, such as phishing and the use of default credentials.
- The list of tools and techniques used to conduct common attacks are constantly changing.
- Many organizations exhibited the same weaknesses.

ATTACK PATH ANALYSIS

CISA developed the following sample attack path, based loosely on the ATT&CK methods used by the assessment teams and the varying success rates of each tactic and technique. Although the sample attack path is not all-encompassing of the potential steps used by threat actors—and not all attack paths follow this model—a skilled threat actor could follow this path to successfully exploit its target. The sample attack path steps serve to highlight the more successful attack strategies used during RVAs and the impacts these strategies have had on target networks.



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 retain *Persistence* [TA0003] on the network. Using the initial foothold within the network, the attacker will use *Privilege Escalation* [TA0004] to gain administrative rights. Then the attacker will use *Defense Evasion* [TA0005] to avoid detection, allowing the attacker to try and steal access with *Credential Access* [TA0006]. Once the attacker has credential access, they will *Discover* [TA0007] the systems and networks to gain an understanding of the infrastructure. After understanding the network, they will use *Lateral Movement* [TA0008] throughout the network and access sensitive data. Once entrenched in the network, the focus of the path switches to the *Collection* [TA0009] of sensitive data. Attackers use *Command and Control* [TA0011] to keep communication channels open to support data *Exfiltration* [TA0010] and potential control after the attack.

Finally, to provide additional context to the attack methods discussed, CISA has chosen the Advanced Persistent Threat (APT) Group 28[2] to highlight a real-world demonstration of how each step is enacted. APT28 is a Russian state sponsored threat actor known for using effective tactics, such as spear-phishing, credential harvesting, and known vulnerability exploitation, to gain access to networks and systems. Russian state-sponsored cyberattacks target a variety of industries, from cleared defense contractors to critical infrastructure.

INITIAL ACCESS

WHAT

Initial Access [TA0001] is the phase of malicious activity during which threat actors attempt to obtain unauthorized access to a victim's internal network. Threat actors can use techniques such as targeted spear-phishing or exploiting weaknesses on public-facing web servers to gain a foothold within a network. During initial access, threat actors typically use techniques that allow some level of anonymity. Initial access is often conducted a "safe" distance from the target, such as from within the attacker's country of origin, but there are many instances of adversaries gaining network access through insider threat or from locally planted media (i.e., CD, DVD, USB, etc.) that contains malicious code. Once initial access has been achieved, threat actors may establish continued access mechanisms, such as valid accounts.

WHY

Gaining initial access to an organization's network is one of the primary goals of an adversary in determining the success of their campaign. If initial access is established undetected, adversaries may have ample time to steal sensitive information, pacing themselves to avoid triggering network detections and alarms. Preventing initial access should be one of the main goals of organizations to protect their network assets and organizational data.

HOW

Threat actors use a variety of attack paths, such as valid accounts or phishing, to gain access to a victim's network. RVA analyses revealed that valid accounts were the most common successful attack technique, responsible for 51 percent of successful attempts to gain initial access. Valid accounts can be previous employee accounts that have not been removed from the active directory or default administrator accounts. When organizations do not change default passwords, they can compromise a valid administrator account. In many cases, this attack technique was possible because the valid account allowed for insecure software (such as unpatched or out of date software) to be installed on or executed on a system or network.

The second most common successful attack technique was phishing. Phishing is the delivery of targeted emails, which often include malicious links or attachments, designed to give the adversary an entryway into the recipient's computer. RVA analyses revealed that phishing links were successful 36 percent of the time. An

[2] APT28, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127, Group G0007 | MITRE ATT&CK®

adversary's success rate with this type of attack will depend 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.

APT28 and other threat actors gain initial access by sending spear-phishing emails with links embedded with malware to steal legitimate credentials and gain access. Once the legitimate credentials are compromised, APT28 will establish a foothold to maintain access and exfiltrate data from a victim's network. During APT28's hacking campaigns, they typically use common tools to remain active on networks and exfiltrate data.

Impact

In many ways, successful entry is the first win achieved by a malicious actor. With internal access, attackers are privy to private systems and information. The next step for the attack, whether it be code execution, mission disruption, or gaining increased privileges, may not be possible without this initial access.

Mitigation/Remediation

- Enable multi-factor authentication (MFA).
- Require strong, unique passwords.
- Enable password management functions.
- Implement time-out and lock-out features.
- Configure time-based access for accounts set at the admin level or higher.
- Create a centralized log management system.
- Ensure applications do not utilize hard-coded passwords.
- Develop and maintain a robust account management policy that includes standards for privileged account management, user training, and password policies.

EXECUTION

WHAT During execution, threat actors deploy various tools needed to conduct the attack by executing malicious code. The malicious code can be executed on the network or systems (local or remote) as an entry method to eventually exfiltrate data.

WHY Threat actors leverage malicious code to execute on systems and networks, further compromising victims. Malicious code can be executed for a variety of reasons, such as establishing backdoors, modifying account privileges, or infecting multiple devices on a network. Threat actors rely on techniques such as executing malicious code to maintain access and control in systems and networks.

HOW Threat actors use a variety of techniques to execute on networks and systems. The CISA Assessments team used "mshta," which is a windows binary designed to execute Microsoft HTML application files. "Mshta" made up 13 percent of the CISA

assessment team's successful execution techniques. Additionally, the CISA Assessments team leveraged PowerShell to successfully discover information and execute code in 12 percent of instances. Threat actors, such as APT28, download and execute PowerShell scripts to run PowerShell commands and run payloads, to further compromise systems and networks.

Impact

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

Mitigation/Remediation

- Disable or remove any unnecessary or unused shells or interpreters.
- Deploy an anti-virus or anti-malware program.
- Restrict web-based content through script blockings.
- Use application control where necessary.

PERSISTENCE

WHAT An ongoing engagement requires an attacker to maintain a foothold in a target network for an extended period. Often, threat actors will use persistence techniques, such as changing credentials or changing system configurations to match their own needs, to maintain their foothold in the system.

WHY Persistence in a network is important for threat actors because it provides time to identify the data they would like to compromise/collect. It also provides time to 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 CISA Assessments team used valid accounts in 72 percent of instances. Valid accounts can be used to bypass access controls placed on various resources across systems within the network and may even be used for persistent access to remote systems and externally available services, such as virtual private networks (VPNs), Outlook Web Access (OWA), and remote desktop. In addition to valid accounts, the CISA Assessments team also used account manipulation to maintain access on the network. During account manipulation, threat actors can modify credentials, permission groups, or network access to subvert security policies.

APT28 is known for compromising accounts to gain access to networks. To remain persistent on the network, APT28 uses "eviltoss," a backdoor that allows it to remain undetected on the network.

Impact

When threat actors are persistent on a network, it allows attackers to re-infect machines 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.

Mitigation/Remediation

- Configure account use policies, such as login times.
- Establish a user account management program monitoring the creation, modification, use and permissions associated to user accounts.
- Enforce privileged account management by managing the creation, modification, use and permissions associated to privileged accounts.

PRIVILEGE ESCALATION

WHAT Typically, threat actors gain initial access through a standard user account, which often has limited access to information. To ensure successful exploitation and compromise, threat actors frequently need to increase the privilege level being used, prior to conducting internal attacks.

WHY Many of the methods used to gain initial access are aimed at any individual working for the organization. Victims can be unaware users or targets of opportunity. Since threat actors target any victim, attackers often begin internal activities with basic user access. To carry out successful operations, threat actors need to escalate privileges to explore networks or access sensitive data.

HOW Threat actors use a variety of tools, such as Windows Credential Editor and ProcDump, to escalate privileges and have system/root-level access or establish administrator-level access. The CISA Assessment team escalated privileges using a valid administrator account in 47 percent of instances. Use of valid administrator accounts can be achieved through multiple means, such as hard-coded credentials, default credentials, or guessed passwords from operating system hash dumps. In addition to valid accounts, the CISA Assessments team successfully injected malicious code into existing processes on 19 percent of successful escalation attempts. Threat actors utilize process injection to evade process-based defenses. Threat actors, such as APT28, utilize publicly available tools (e.g., “Mimikatz,” a source code used to collect credentials) to carry out their operations. Threat actors often use these tools in conjunction with system-level privileges to gain access to enterprise-level accounts, such as domain administrator.

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, for example, could impair mission-critical functions, potentially leading to the loss of equipment or resources.

Mitigation/Remediation

- Enable MFA.
- Require strong, unique passwords.
- Enable password management functions.
- Ensure applications do not utilize hard-coded passwords.
- Develop and maintain a robust account management policy that includes standards for privileged account management, user training, and password policies.
- Change default passwords to meet approved password policy.
- Consider deploying endpoint security solutions with the ability to prevent process injection.
- Restrict user accounts to least privilege to limit administrative access to tokens.
- Limit user and user group permissions to token creation through group policy object (GPO).
- Maintain proper authentication and authorization standards.

DEFENSE EVASION

WHAT Threat actors try to navigate systems and networks undetected for as long as possible. They utilize defense evasion techniques to avoid detection during attack. Defense evasion techniques include disabling security software or obfuscating data.

WHY Defense evasion techniques enable threat actors to navigate throughout networks and systems for longer periods of time, without being noticed by the victim. Defense evasion techniques do not require significant resources. They can be simple techniques, such as deleting files or masquerading. The longer an adversary goes unnoticed on the system or network, the longer the adversary can carry out operations.

HOW Threat actors utilize different defense evasion techniques, from disabling security software to cross-site scripting. The CISA Assessment team utilized valid accounts in 25 percent of instances of defense evasion. The use of valid accounts allowed them to go unnoticed on the network for extend periods of time. Additionally, the CISA Assessments team used “mshta” in 13 percent of instances; the team used the “mshta.exe” to proxy execution of malicious “.hta” files and Javascript or VBScript through a trusted Windows utility.

Some threat actors may exploit systems or application vulnerabilities to bypass security features by taking advantage of a programming error or disabling security

software. APT28 obfuscates files using the macro command “certutil -decode” to decode the contents of a “.txt” file storing the “base64” encoded payload.

Impact

If threat actors can remain on networks undetected for extended periods of time, they can cause serious damage. When threat actors go undetected, they can access and exfiltrate large amounts of data and disrupt daily operations.

Mitigation/Remediation

- Enable a threat intelligence program to quickly identify abnormal activity.
- Update software frequently to avoid vulnerabilities.
- Implement exploitation protection.

CREDENTIAL ACCESS

WHAT Threat actors steal credentials to gain access to internal resources, bypass security measures, and steal critical data.

WHY Using legitimate credentials can give adversaries access to systems, can make their movements and activities harder to detect, and can allow them to create more accounts to help achieve their goals.

HOW Threat actors use a variety of techniques to steal credentials, such as keylogging or credential dumping. In 20 percent of assessments, the CISA Assessments team successfully spoofed an authoritative source for name resolution to force communication with an assessment 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 CISA Assessments team leveraged credentials discovered in files in 15 percent of instances. Threat actors, such as APT28, use brute force attacks and password spraying techniques to obtain credentials.

Impact

If threat actors have access to privileged credentials, they can escalate privileges, access sensitive data, and bypass security controls.

Mitigation/Remediation

- Enable MFA.
- Enforce password policies.
- Establish user account management.
- Set account lockout policies and failed number of login attempts.

DISCOVERY

WHAT Threat actors steal credentials to gain access, bypass security measures, and steal

WHAT Discovery is an important phase for the attacker. During discovery, the threat actor is trying to learn about the network, systems, and data.

WHY 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. During discovery, the threat actor can 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 accounts on a system or within the network that will be of use, such as privileged accounts. The CISA Assessments team leveraged account discovery techniques in 9 percent of instances to identify accounts that would be beneficial in accessing sensitive data. To further identify information, the CISA Assessments team used network share discovery in 8 percent of instances to access folders and drives of interest for collection.

Threat actors, such as APT28, rely on other techniques, such as network sniffing, to capture information about the environment. APT28 is known for deploying Responder, an open-source tool, to conduct NetBIOS Name Service poisoning, which captured usernames and hashed passwords that allowed access to legitimate credentials.[3]

Impact

During discovery, threat actors gain context to a victim's network. Threat actors can gain an understanding of important accounts, the network, and assets, as well as access to critical data. It is important to deploy the proper safeguards to ensure cyber actors cannot easily access critical systems and data.

Mitigation/Remediation

- Enable MFA.
- Encrypt Sensitive Information.
- Monitor operating system configurations.
- Audit network activity to identify abnormal behavior.
- Employ network segmentation for sensitive domains.

[3] Discovery, Tactic TA0007 - Enterprise | MITRE ATT&CK®

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. These activities are conducted after initial access is obtained and are often used to move to network locations of specific interest to the adversary.

WHY Threat actors often 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 through the environment. Adversaries move through the network from host to host, or account to account, until they can reach the location within the target environment necessary to conduct further attack steps.

HOW To laterally move throughout the network, threat actors might use their own remote access tools or compromised credentials. The CISA Assessments team used Pass the Hash (PtH) in 27 percent of instances to laterally move through the network. This technique bypasses the step of supplying account passwords, by submitting the password hashes to the authentication process. PtH may provide adversaries authenticated access to systems without discovering the compromised user account's password. In addition to PtH, the CISA Assessments team utilized Remote Desktop Protocol in 18 percent of instances to expand their footprint within the compromised network by remotely accessing and controlling neighboring hosts from previously exploited systems.

Threat actors, such as APT28, use many different techniques to laterally move throughout the network. APT28 has used CVE-2015-1701, Win32k Elevation of Privilege Vulnerability, which allows local users to gain privileges through a crafted application and exploit. They have also leveraged techniques such as PtH to laterally move throughout the network. APT28 can use stolen password hashes to move laterally within an environment, bypassing normal system access controls.

Impact

Many organizations' networks house systems or data deemed critical to achieving overall mission success. These systems are typically located in network segments with increased protections, and access is oftentimes restricted based on user roles and privilege level. However, by allowing a threat actor to pivot from host to host within a compromised environment, critical systems may become accessible. Limiting an adversary's lateral movement constrains their activity to a confined space, potentially preventing their ability to meet their target objectives.

Mitigation/Remediation

- Limit credential overlap across systems (e.g., Windows Local Administrator Password Solution).

- Ensure sensitive data is not on shared files by running monthly scans to look for password files or config files with similar data.
- Do not allow a domain user to be in the local administrator group on multiple systems.
- Apply appropriate Windows patches and configurations (e.g., pass-the-hash mitigations: apply user account control restrictions to local accounts on network logons).
- Use MFA for remote management sessions.
- Disable the remote desktop protocol (RDP) service if it is unnecessary.
- Routinely review the list of users with remote management privileges and remove unnecessary accounts.
- Limit use of remote services.
- Use application isolation and sandboxing techniques to increase network segmentation, limiting unauthorized movement.
- Use host-based firewall rules to limit host-to-host traffic to required protocol and services.

COLLECTION

WHAT After threat actors establish a presence within an organization's network, they can begin to collect sensitive internal data for a variety of reasons, such as competitive advantage or espionage. Many threat actors gather information through a variety of techniques, such as capturing screenshots and keyboard inputs.

WHY It is important for threat actors to collect data from victims' networks. Data collection can assist threat actors with intelligence or surveillance efforts for future operations, or it can help threat actors gain financial advantages. Ultimately, data collection is key to successful malicious operations.

HOW Collection can be carried out through a variety of means. The CISA Assessments team revealed that data on shared drives constituted 33 percent of successful data access attempts. Network shares are often used to segment data for role-based access, such as admin shares. Network shares weaknesses exist when users who should not be able to view specific data are granted access to shares due to misconfigured permissions. Additionally, the CISA Assessments team also obtained sensitive data from local systems in 29 percent of instances. The CISA Assessments team was able to locate local file systems and databases, enabling them to access sensitive information.

Threat actors, such as APT28, rely on properly collecting, exfiltrating, and archiving data. APT28 is known for using publicly available tools, such as WinRAR, to archive collected data with password protection.

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.

Mitigation/Remediation

- Unfortunately, data collection cannot be directly remediated.
- Any activity conducted during collection utilizes existing system features, such as operating system directory structure or database queries. Implement defenses that limit the effectiveness of attack phases leading up to and following data collection.
- Monitor network effectively to detect collection efforts; use of honey tokens or honey files will alert network defenders to malicious collection attempts.
- Deploy data loss prevention (DLP) tools to detect and alert to unauthorized data access.
- Ensure the proper preventative controls are in place.

COMMAND AND CONTROL (C2)

WHAT An ongoing engagement requires an attacker to maintain a foothold in a target network for an extended period. Threat actors will attempt to create an avenue to allow themselves continued access to the environment at any given moment. By establishing a hidden communications channel between their remote servers and compromised systems within the target network, adversaries can conduct internal activity while avoiding detection.

WHY Depending on the overall intent of a malicious campaign, attacks may span the course of several weeks or months. Attackers operating at remote locations need prolonged, undetected access to targeted systems to identify and collect sensitive data and quietly disrupt day-to-day operations.

HOW Threat actors use C2 techniques to communicate with compromised systems. The CISA Assessments team deployed C2 channels utilizing non-standard ports in 15 percent of their successful attempts. Passing data through ports not commonly associated with the protocol being used is a common tactic for evading detection or bypassing network filters. Additionally, techniques such as hiding C2 traffic within legitimate network traffic made up 14 percent of successful C2 methods used in RVAs.

APT28 will leverage C2 techniques to communicate with systems under control within a victim network by mimicking existing traffic and using the application layer protocol. APT28 is also known for sending malware over the C2 server.

Impact

The use of undetected control channels to conduct operations remotely, from anywhere in the world, allows adversaries the anonymity and stealth needed to operate on a victim network, uninterrupted until their mission objectives are achieved.

Mitigation/Remediation

- Utilize firewall rules to limit outgoing traffic to required protocols.

- Use signature-based intrusion detection system (IDS)/intrusion prevention system (IPS) devices to identify known bad network activity.

EXFILTRATION

WHAT Threat actors use a variety of exfiltration techniques to steal data from victims' networks. Threat actors target sensitive information such as blueprints, security requirements documents, or vulnerability information from a compromised system or enclave.

WHY Many adversaries conduct attacks to gain access to information such as financial information, sensitive security data, or personally identifiable information. By removing this data, adversaries may be able to analyze organizational information from the safety of their remote location. Even if their activity is detected by the compromised organization and their campaign is ended, the stolen data is still available to the attacker for later use.

HOW Threat actors use a variety of techniques to exfiltrate data. The CISA Assessments team successfully exfiltrated data over the C2 channel in 66 percent of instances. Using the C2 channel established for remote access allowed the CISA Assessments team to download information without establishing additional pathways and potentially alerting network defenders.

Adversaries, such as APT28, will package and compress data to exfiltrate undetected by using archives of data from the victim's OWA server via HTTPS or over Google Drive.

Impact

Threat actors 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 customers, or disrupt day-to-day operations.

Mitigation/Remediation

- Deploy network intrusion detection/prevention systems to alert or stop network traffic associated with known malware; at network boundaries, IDS and IPS protections use signature-based analysis to determine if traffic is malicious.
- Implement SSL decryption for web proxies and ensure all internet traffic flows through this mechanism; monitor cleartext traffic for unusual activities.
- Deploy DLP tools to detect and alert to unauthorized data removal.

CONCLUSION

The CISA Assessment team conducted 112 RVAs intended to assess the participating entities' network capabilities and network defenses against potential threats. After conducting trend analysis on entities' networks and network defenses, CISA had several high-level observations from enhanced security to patching outdated software.

During the initial access phase, many organizations fell victim to common access methods, such as phishing and the use of default credentials. This demonstrates that initial attack vectors have not changed over time and that organizations should continue to implement enhanced password protection practices. Since attack vectors have not changed and remain successful, all sectors should focus on enhancing password requirements, implementing user training to identify phishing, and requiring password changes after a set period.

Network defenders should remain vigilant to threat actors' evolving tactics and techniques. To help quickly identify abnormal activity, network defenders should continuously review intrusion detection systems and logs to identify adversary activity. During its RVAs, CISA was able to escalate privilege and laterally move throughout entities' networks, gaining access to sensitive information. If entities can quickly identify malicious activity, they can reduce the impact of compromise.

Lastly, CISA observed that many organizations across multiple sectors exhibited similar weaknesses, such as a prevalence of default passwords, open ports, and outdated software. CISA recommends all industries practice strong password management to reduce the risk of compromise, patch outdated software, and close inactive ports. In addition to the recommendations and mitigations provided after each section, CISA recommends individual organizations create additional tailored guidance to fit their specific network architectures, while dealing with their specific resource constraints. CISA encourages system owners and administrators to convey its 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 agencies.

REFERENCES

- The MITRE Corporation, *MITRE ATT&CK,* Retrieved from https://attack.mitre.org
- The MITRE Corporation, *APT28*, Retrieved from https://attack.mitre.org/groups/G0007/
- National Institute of Standards and Technology, *National Vulnerability Database*, Retrieved from https://nvd.nist.gov