TLP:WHITE

CISA Analysis: FY2020 Risk and Vulnerability Assessments

Publication: July 2021

TLP:WHITE

BACKGROUND

Each year, the Cybersecurity and Infrastructure Security Agency (CISA) conducts Risk and Vulnerability Assessments (RVAs) of Federal Civilian Executive Branch (FCEB), Critical Infrastructure (CI), and State, Local, Tribal, and Territorial (SLTT) stakeholders. An RVA assesses an organization's overall effectiveness in identifying and addressing network vulnerabilities. In Fiscal Year 2020 (FY20), CISA conducted 37 RVA assessments of multiple stakeholders across the various sectors and aligned the results to the MITRE ATT&CK® framework. The goal of the RVA analysis is to develop effective strategies that positively impact the security posture of FCEB, SLTT, and CI stakeholders.

During an RVA, CISA collects data through onsite assessments and combines it with national threat and vulnerability information to provide an organization with actionable remediation recommendations prioritized by risk. CISA designed RVAs to identify vulnerabilities that adversaries could exploit to compromise network security controls. An RVA 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 the RVA, CISA provides the organization a final report that includes business executive recommendations, specific findings, potential mitigations, and technical attack path details.

CISA's RVA teams leverage the MITRE ATT&CK framework, which is a **"**globally accessible knowledge base of adversary tactics and techniques based on real-world observations."[1] The framework aims to build a community-driven knowledge base—comprising known tactics, techniques, and procedures (TTPs) of threat actors—to help develop threat models and facilitate vulnerability mitigation efforts. The framework includes 14 distinct attack paths that cyber adversaries use to obtain and maintain unauthorized access to a network/system.

[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 with weaknesses that are representative of those CISA observed in the FY20 RVAs.[2] The path comprises six successive tactics, or "steps": *Initial Access*, *Command and Control*, *Lateral Movement*, *Privilege Escalation*, *Collection*, and *Exfiltration*. In addition to this analysis, the report includes the following observations:

- Most of the successful attacks proved to be methods commonly used by threat actors, e.g., phishing, use of default credentials.
- The list of tools and techniques used to conduct these common attacks is ever changing.
- Many of the 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. Considering the most successful methods, it is reasonable to assume that a skilled threat actor may follow this path to successfully exploiting its target.

This path is not all-encompassing of the potential steps used by malicious actors and not all attack paths follow this model. However, these steps serve to highlight some of the more successful attack strategies used during RVAs and the impacts these strategies have had on a target network.

The attack path begins with a step required by many real-world attacks: gaining *Initial Access* [TA0001]. Next in the path is establishing *Command and Control* [TA0011]. Using the initial foothold within the network, *Lateral Movement* [TA0008] is conducted, followed by attempts at *Privilege Escalation* [TA0004]. Once entrenched in the network, the focus of our path switches to the *Collection* [TA0009] of sensitive data and concludes with *Exfiltration* [TA0010].

Note: This attack path does not directly align with the techniques and methods used by the RVA teams. See Figure 1 for tactic icons used in this report.

[2] See https://www.cisa.gov/publication/rva for the FY20 infographic: *RVAs Mapped to the MITRE ATT&CK Framework*, which breaks out the top three most successful techniques for each tactic documented by the FY20 RVAs.

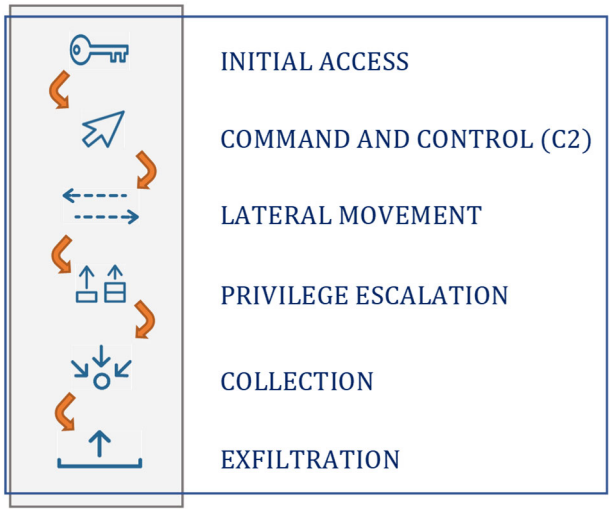

Figure 1: Tactic Icons

A thorough analysis of vulnerability trends (i.e., prevalence over time, types of systems and agencies impacted, etc.) includes an examination of the impact the vulnerabilities have on affected systems. The below attack path analysis includes an **Impact** section for each tactic that details the possible results of successful exploitation.

Additionally–because awareness of critical vulnerabilities alone does not successfully improve security posture—the analysis includes a **Mitigation/Remediation** section for each tactic, which details mitigations/remediations for the vulnerabilities associated with each attack strategy.

Finally, to provide more context to the attack methods discussed and highlight how each tactic is enacted, the analysis includes known TTPs associated with Advanced Persistent Threat (APT) group APT39.[3] An examination of real world, adversarial TTPs can aid vulnerability analysts in determining the actual effectiveness of current and future network protections and help prioritize mitigation activities.

INITIAL ACCESS

WHAT *Initial Access* [TA0001] is the step during which cyber threat actors attempt to obtain unauthorized access to a victim organization's internal network. These attacks depend on remotely positioned adversaries gaining internal access to an organization's network. Typically involving techniques that allow some level of anonymity, access steps are often conducted from a "safe" distance from the target, such as the attacker's country of origin. However, there are many instances of adversaries gaining network access through an insider threat or from locally planted media (e.g., CD, DVD, USB) containing malware.

WHY Gaining initial access to an organization's network is one of the primary goals of a threat actor in determining the success of their campaign. If initial access is established undetected, threat actors may have ample time to steal sensitive information, pacing

[3] Although APT39's targeting scope is global, its activities are concentrated in the Middle East. Masked behind its front company, Rana Intelligence Computing Company (Rana), the Government of Iran employed a years-long malware campaign that targeted Iranian dissidents, journalists, and international companies in the travel sector.

themselves to avoid triggering network detections and alarms. Preventing initial access should be one of the primary goal organizations establish to protect their network assets and to keep sensitive information intact.

HOW

APT39 uses a variety of custom and publicly available malware and tools at all stages of the attack lifecycle. APT39 has sent spearphishing emails with malicious attachments (*Phishing: Spearphishing Attachment* [T1566.001]) or hyperlinks (Phishing: Spearphishing Link [T1566.002]), typically resulting in a POWBAT infections. In addition to using a specific variant of the POWBAT backdoor, APT39 has primarily leveraged the SEAWEED and CACHEMONEY backdoors. APT39 also used attack techniques such as SQL Injection (*Exploit Public-Facing Application* [T1190]) to gain a foothold on public-facing applications. After compromising web servers, APT39 has proceeded to install web shells, such as ANTAK and ASPXSPY, and has used stolen, legitimate credentials to compromise externally facing Outlook Web Access (OWA) resources (*Server Software Component: Web Shell* [T1505.003]).

RVA Attack Analysis

Phishing: While conducting assessments, the RVA team obtained initial access using phishing links [T1566.002] 49 percent of the time and phishing attachments [T1566.001] 9.8 percent of the time. Phishing is the delivery of targeted emails that often include malicious links or attachments designed to provide the adversary an entryway into the recipient's computer. An adversary's phishing success rate depends on multiple 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.

Exploit Public-Facing Applications: Attacks on public-facing applications made up 11.8 percent of successful attempts at gaining initial entry during RVAs. This type of attack involves exploiting the vulnerabilities associated with applications that are accessible from the internet. The existence of these vulnerabilities is typically public knowledge and, as a result, there may be several active exploits or proof of concepts (POCs) associated with them. Targets for these attacks include websites, databases, and network services (e.g., Secure Shell [SSH], Telnet, File Transfer Protocol [FTP]).

Valid Accounts: The use of legitimate accounts made up 11.8 percent of successful attempts at gaining initial entry during RVAs. In many cases, gaining initial access through valid accounts is made possible via insecure software development practices. Examples include hard-coded passwords in web application code, default credentials for well-known applications, and unintentional information disclosure of account information on public forums or open-source code repositories.

Impact

Successful entry is often 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 lateral movement, mission disruption, or gaining increased privileges—may not be possible without this initial access.

Mitigation/Remediation

- Control execution through allowed application lists.

- Disable macros.
- Monitor the execution of Living Off the Land Binaries (LOLBins).
- Identify and remediate public facing vulnerabilities to help prevent initial access using a proactive patch management program.
- Train users to be aware of suspicious emails as well as the common indicators of social engineering attempts.
- Utilize a cloud service provider for mail exchange (MX) that implements strong email security, including Domain-based Message Authentication, Reporting and Conformance (DMARC), Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and attachment vulnerability scanning.
- Used together, these technologies form a strong anti-phishing mechanism for an organization's mail exchange.
- Implement—if a cloud provider is not an option—an email technology that will:
    - sandbox or review email attachments for any malicious functionality, and
    - review email messages for malicious external links and domains.

COMMAND AND CONTROL (C2)

WHAT An ongoing engagement requires an attacker to maintain a foothold in a target network for an extended period. An attacker 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 Some adversaries require a great deal of time with exposure to the victim environment. Depending on the overall intent of a malicious campaign, attacks may span several weeks or months. The time needed to slowly identify and collect sensitive data, or quietly disrupt day-to-day operations, requires undetected access to target systems while operating from remote locations.

HOW One common method for establishing a command and control tunnel into and out of a compromised network is to send all traffic through a well-known port or protocol. APT39 has used tools that communicate with common protocols—such as HTTP and DNS—that routinely pass back and forth between the internet and internal network segments. Additionally, APT39 has used tools that masquerade as legitimate applications to evade detection of control communication. For example, applications posing as Mozilla Firefox or McAfee components often go undetected.

RVA Attack Analysis

Web Protocols: Most of the successful attempts at establishing communication channels from within the assessed organization's network utilized ports that are typically associated with standard communication protocols. This use of well-known ports and protocols comprised 42 percent of successful attempts at establishing C2. By using a protocol that is typically allowed through boundary protections, such as HTTP or DNS, the assessment teams can evade common port filtering and potentially avoid detection.

Remote Access Software: The assessment teams used remote tools (15.9 percent of successful attempts) such as the Microsoft Windows Remote Desktop Protocol (RDP) to discretely manage

internal activity and to spread their attack footprint to neighboring systems. The use of known remote management tools can allow attackers to avoid perimeter protocol filters.

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 mission objectives are achieved.

Mitigation/Remediation

- Prevent applications from storing credential data and change default usernames and passwords where applicable.
- Periodically review user and application privilege level and search for newly created accounts to identify unauthorized grants of elevated privilege.
- Configure firewalls with granular ingress and egress rules, which not only prevent remote access applications from communicating outside of the network, but also allow only protocols required by the communicating network segment to exit.
- Deploy signature-based intrusion detection/prevention (IDS/IPS) systems to identify malicious communications traffic at both the network and host levels.
- Configure systems to prevent the installation and execution of unauthorized applications.
- Utilize web proxies to limit use of external web services.
- Implement Secure Sockets Layer (SSL) decryption for web proxies and ensure all internet traffic flows through this mechanism.
- Monitor cleartext traffic for unusual activities.

LATERAL MOVEMENT

WHAT Lateral movement is the process of pivoting from host to host or from one user account to another in order 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 Many times adversaries will gain access to compromised networks without having proximity to the specific systems or data they are targeting. Additionally, the level of privilege they obtain may not be high enough to garner the access they need. For these reasons, it is often necessary for adversaries to laterally move through the network from host to host or account to account until they can reach the location within the target environment needed to conduct further attack steps.

HOW After establishing a communication channel into the target network, APT39 has used SOCKS5 proxies, RDP, and SSH to distribute remote commands throughout multiple compromised hosts. Several of these protocols may also be used to compromise valid accounts via session hijacking. Several other well-known, built-in protocols have been used to attack additional hosts within the target network. For example, APT39 has used Server Message Block (SMB) to access network shares to potentially transfer and execute malicious binaries on neighboring hosts.

RVA Attack Analysis

Pass the Hash (PtH): PtH made up 29.8 percent of successful RVA attempts at lateral movement. 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.

Remote Desktop Protocol (RDP): The use of RDP (25 percent of successful attempts at lateral movement) allowed the assessment teams to expand their footprint within compromised networks by remotely accessing and controlling neighboring hosts from previously exploited systems.

Exploitation of Remote Services: Remote services exhibiting coding errors were exploited from within the compromised network (11.9 percent of successful attempts at lateral movement). In some cases, the privilege level of the exploited service is higher than that of the adversary. Exploiting remote services with heightened privileges may result in increased privilege levels on the newly compromised system.

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 typically restricted based on user roles and privilege level. However, by allowing an adversary to pivot from host to host within a compromised environment, it is possible for these critical systems to become susceptible to compromise. 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 share files by running monthly scans 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 Access Control (UAC) restrictions to local accounts on network logons).
- Use multifactor authentication (MFA) for remote management sessions.
- Disable the 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.

PRIVILEGE ESCALATION

WHAT The level of initial access acquired by cyber threat actors is often limited. To ensure successful exploitation and compromise, malicious actors often attempt to increase the privilege level being used prior to conducting internal attacks.

WHY Many of the methods threat actors use to gain initial entry aim to obtain basic user access. For this reason, attackers may begin internal activities with basic user access and seek to escalate their privilege level. Maintaining proper authentication and authorization standards would limit user access to sensitive data, networks segments, and controls. Without control of privileged, administrative, or Root/SYSTEM accounts, adversarial attacks may not succeed.

HOW After the initial foothold has been established, APT39 typically utilizes freely available tools, such as Mimikatz and Ncrack, in addition to legitimate tools, such as Windows Credential Editor and ProcDump, for privilege escalation. APT39 often uses these tools in conjunction with system-level privileges to gain access to enterprise-level accounts such as a Domain Administrator account.

RVA Attack Analysis

Valid Accounts: The assessment teams were able to escalate their level of privileged access during many of the RVA assessments conducted in 2020. The use of legitimate accounts made up the largest portion (37.5 percent) of the successful tactics used. Use of valid accounts can be achieved through various means including hard coded credentials, default credentials, or guessed passwords from operating system hash dumps.

Exploitation for Privilege Escalation: The assessment teams used exploitation techniques on 21.9 percent of their successful attempts at privilege escalation. This form of escalation takes advantage of system or software vulnerabilities that specifically lead to an increased level of user privilege. An example of this type of attack would be to trick a vulnerable application into creating an account for the attacker and granting them elevated privileges.

Token Impersonation: The teams used copies of existing security tokens for 15.6 percent of successful RVA escalation techniques. Using tokens from existing system-level processes, and then attaching these tokens to malicious processes, allows a threat actor to run their code with increased privileges; potentially providing more access and control than administrator accounts (e.g., 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, having Domain Administrator access, for example, could allow a threat actor to impair mission critical functions that could potentially lead to the loss of equipment or resources.

Mitigation/Remediation

- Update software applications regularly.
- Exercise least privilege when creating and managing accounts.
- Limit users' permissions to create tokens.
- Prevent write access to logon scripts and prevent modification of associated registry keys.
- Utilize sandboxes and application micro segmentation where applicable

to limit adversarial movement and exposure.
- Prevent applications from storing credential data and change default username and password where applicable.
- Periodically review user and application privilege level and search for newly created accounts to identify unauthorized grants of elevated privilege.
- Perform password file searches on all shares and local drives.
- Configure applications with security best practice standards (e.g., disable xp_cmdshell on MS SQL Databases).
- Utilize a strong password policy to prevent password hashes from being easily guessed.

COLLECTION

WHAT After achieving a presence within an organizations network, collection of sensitive internal data is often one of the primary goals of an attacker. Attempts to pull this data from within the compromised network using C2 channels may be the next steps in their attack plan.

WHY APT39's significant targeting of the telecommunications and travel industries reflects efforts to collect personal information on targets of interest and customer data for the purposes of surveillance and to facilitate future operations. Telecommunications firms are attractive targets given that they store large amounts of personnel and customer information, provide access to critical infrastructure used for communications, and enable access to a wide range of potential targets across multiple verticals.

HOW Undetected adversaries with an internal foothold and elevated privileges may have access to file systems and directories containing sensitive information, as well as network shares with access typically limited to specific users (e.g. Admin Shares). APT39 has used the tool CrackMapExec to enumerate network shares searching for stores of sensitive data. Once found, APT39 has used tools such as 7-zip and WinRAR to create data archives.

RVA Attack Analysis

Data from Local System: Sensitive information identified by the assessment teams was found primarily on local systems. This sensitive information accounted for 32.2 percent of successful attempts at locating sensitive data. Local file systems and databases are typical sources of local data.

Data from Network Share Drive: The RVA reports revealed that data on shared drives constituted 30.5 percent of successful data access attempts. Network shares are often used to segment data for role-based access, such as Admin shares. Remotely accessing network shares is not a finding itself. The weakness exhibited here exists when users who should not be permitted to view specific data are granted access to shares due to misconfigured permissions.

Impact

Allowing adversaries to locate and collect sensitive data negates the intended function of network security, communication security, operation security, and physical security efforts.

Mitigation/Remediation

- Unfortunately, data collection cannot be directly remediated. Any activity conducted during collection uses existing system features such as operating system directory structure or database queries. For this reason, it is critical that defenses are implemented to limit the effectiveness of the attack phases leading up to and following data collection.
- Effective network monitoring will aid in the detection of collection efforts. Use of honey tokens or honey files will alert network defenders of malicious collection attempts.
- Deploy data loss prevention (DLP) tools to detect and alert on unauthorized data access.

EXFILTRATION

WHAT Some adversaries 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 building plans, IP ranges, software versions, and hardware lists. 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 agency and their campaign is ended, the stolen data is still available to the attacker for later use.

HOW Using either existing C2 channels or hidden within traffic flowing through common ports and protocols–such as HTTPS–attackers can package and send data to various systems on the internet. APT39 has also used the legitimate web service DropBox to conduct C2 for uploading and downloading stolen files and malicious code.

RVA Attack Analysis

Exfiltration over C2 Channel: 68.2 percent of successful exfiltration attempts by the assessment teams was conducted through C2 channels. Using the same channels previously established for remote access allowed the teams to download information without the need for establishing additional pathways and potentially alerting network defenders.

Impact

The analysis of stolen information may lead to the recreation of blueprinted technologies, targeting of supply chain components, or public release of information to achieve other sociopolitical objectives.

Mitigation/Remediation

- Deploy network IDS/IPS to alert or stop network traffic associated with known malware. At the 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 data loss prevention (DLP) tools to detect and provide alerts on unauthorized data removal.

CONCLUSION

After conducting trend analysis on the 37 RVA reports executed by CISA, several high-level observations were identified. Methods such as phishing and the use of default credentials were still viable attacks. This shows that the methodologies used to compromise much of our infrastructure have not changed drastically over time. As a result, network defenders must refocus their efforts at deploying the myriad of mitigation steps already known to be effective.

Unfortunately, the list of tools and techniques used to conduct well-known attacks is constantly evolving. For this reason, network defenders much remain vigilant in understanding and observing the signatures of new TTPs. An additional observation is that for several MITRE categories, many organizations exhibited the same weaknesses. Threat actors, with capability and intent, may be successful at compromising many agencies across multiple sectors. Conversely, the benefit of this trend is that the high-level mitigation recommendations made by CISA may apply to many organizations. However, individual organizations will need to tailor fix guidance to fit their specific network architectures while dealing with their specific resource constraints. CISA strongly recommends system owners and administrators convey this guidance to their leadership and apply changes relevant to the nuances of their specific environments.

Finally, CISA concludes that analysis of this nature may help network defenders—across multiple sectors and organizations—effectively prioritize the identification and mitigation of high-level vulnerabilities. CISA intends for future iterations of this effort to incorporate the specific TTPs used by the assessment teams, which should facilitate a more thorough analysis and potentially improve mitigation recommendations.

REFERENCES

- CISA Cyber Resource Hub. https://www.cisa.gov/cyber-resource-hub.
- CISA RVA webpage. https://www.cisa.gov/publication/rva.
- MITRE ATT&CK. https://attack.mitre.org.
- MITRE ATT&CK v9.0, Enterprise Tactics. https://attack.mitre.org/versions/v9/tactics/enterprise/.
- The MITRE Corporation (2015), *APT 39*. https://attack.mitre.org/groups/G0087/.
- National Institute of Standards and Technology, *National Vulnerability Database*. https://nvd.nist.gov.