America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

CYBERSECURITY ADVISORY

CISA Red Team's Operations Against a Federal Civilian Executive Branch Organization Highlights the Necessity of Defense-in-Depth

Release Date: July 11, 2024 **Alert Code:** AA24-193A

RELATED TOPICS: CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE </topics/critical-infrastructure-security-and-resilience>, CYBERSECURITY BEST PRACTICES </topics/cybersecurity-best-practices>, INCIDENT DETECTION, RESPONSE, AND PREVENTION </topics/cyber-threats-and-advisories/incident-detection-response-and-prevention>

EXECUTIVE SUMMARY

In early 2023, the Cybersecurity and Infrastructure Security Agency (CISA) conducted a SILENTSHIELD red team assessment against a Federal Civilian Executive Branch (FCEB) organization. During SILENTSHIELD assessments, the red team first performs a no-notice, long-term simulation of nation-state cyber operations. The team mimics the techniques, tradecraft, and behaviors of sophisticated threat actors and measures the potential dwell time actors have on a network, providing a realistic assessment of the organization's security posture. Then, the team works directly with the organization's network defenders,

system administrators, and other technical staff to address strengths and weaknesses found during the assessment. The team's goal is to assist the organization with refining their detection, response, and hunt capabilities—particularly hunting unknown threats.

In coordination with the assessed organization, CISA is releasing this Cybersecurity Advisory (CSA) detailing the red team's activity and tactics, techniques, and procedures (TTPs); associated network defense activity; and lessons learned to provide network defenders with recommendations for improving their organization's detection capabilities and cyber posture.

During the first phase, the SILENTSHIELD team gained initial access by exploiting a known vulnerability in an unpatched web server in the victim's Solaris enclave. Although the team fully compromised the enclave, they were unable to move into the Windows portion of the network due to a lack of credentials. In a parallel effort, the team gained access to the Windows network through phishing. They then discovered unsecured administrator credentials, allowing them to pivot freely throughout the Windows environment, which resulted in full domain compromise and access to tier zero assets. The team then identified that the organization had trust relationships with multiple external partner organizations and was able to exploit and pivot to an external organization. The red team remained undetected by network defenders throughout the first phase.

The red team's findings underscored the importance of defense-in-depth and using diversified layers of protection. The organization was only able to fully understand the extent of the red team's compromise by running full diagnostics from all data sources. This involved analyzing host-based logs, internal network logs, external (egress) network logs, and authentication logs.

The red team's findings also demonstrated the value of using tool-agnostic and behavior-based indicators of compromise (IOCs) and of applying an "allowlist" approach to network behavior and systems, rather than a "denylist" approach, which predominantly results in an unmanageable amount of noise. The red team's findings illuminated the following lessons learned for network defenders about how to reduce and respond to risk:

- **Lesson learned:** The assessed organization had insufficient controls to prevent and detect malicious activity.
- **Lesson learned:** The organization did not effectively or efficiently collect, retain, and analyze logs.
- **Lesson learned:** Bureaucratic processes and decentralized teams hindered the organization's network defenders.
- **Lesson learned:** A "known-bad" detection approach hampered detection of alternate TTPs.

To reduce risk of similar malicious cyber activity, CISA encourages organizations to apply the recommendations in the Mitigations section of this advisory, including those listed below:

- **Apply defense-in-depth principles** by using multiple layers of security to ensure comprehensive analysis and detection of possible intrusions.
- **Use robust network segmentation** to impede lateral movement across the network.
- **Establish baselines of network traffic, application execution, and account authentication**. Use these baselines to enforce an "allowlist" philosophy rather than denying known-bad IOCs. Ensure monitoring and detection tools and procedures are primarily behavior-based, rather than IOC-centric.

CISA recognizes that insecure software contributes to these identified issues and urges software manufacturers to embrace Secure by Design <https://www.cisa.gov/securebydesign> principles and implement the recommendations in the Mitigations section of this CSA, including those listed below, to harden customer networks against malicious activity and reduce the likelihood of domain compromise:

- **Eliminate default passwords.**
- **Provide logging at no additional charge**.
- **Work with security information and event management (SIEM) and security orchestration, automation, and response (SOAR) providers**—in conjunction with customers—to understand how response teams use logs to investigate incidents.

Download the PDF version of this report:

AA24-193A CISA Red Team's Operations Against a Federal Civilian Executive Branch Organization Highlights the Necessity of Defense-in-Depth </sites/default/files/2024-07/csa-cisa-red-team%27s-operations-against-a-fceb-organization-highlights-the-necessity-of-defense-in-depth_0.pdf>

(PDF, 1.18 MB)

AA24-193A CISA Red Team's Operations Against a Federal Civilian Executive Branch Organization Highlights the Necessity of Defense-in-Depth - Spanish Translation </sites/default/files/2024-10/csa-cisa-red-team_s-operations-against-a-fceb-organization-highlights-the-necessity-of-defense-in-depth_0_es.pdf>

(PDF, 1.06 MB)

INTRODUCTION

CISA has authority to hunt for and identify, with or without advance notice to or authorization from agencies, threats and vulnerabilities within federal information systems (see generally 44 U.S.C. § 3553[b][7]). The target organization for this assessment was a large U.S. FCEB organization. CISA conducted the SILENTSHIELD assessment over an approximately eight-month period in 2023, with three of the months consisting of a technical collaboration phase:

- **Adversary Emulation Phase:** The team started by emulating a sophisticated nation-state actor by simulating known initial access and post-exploitation TTPs. The team's goal was to compromise the assessed organization's domain and identify attack paths to other networks. After completion of their initial objectives, the team diversified its deployed tools and tradecraft to mimic a wider and often less sophisticated set of threat actors to elicit network defender attention. CISA red team members did not clean up or delete system logs, allowing defenders to investigate all artifacts and identify the full scope of a breach.

- **Collaboration Phase:** The SILENTSHIELD team met regularly with senior staff and technical personnel to discuss issues with the organization's cyber defensive capabilities. During this phase, the team:
  - Proposed new behavior-based and tool-agnostic detections to uncover additional tradecraft used during the Adversary Emulation Phase. They also evaluated the organization's improvements according to current CISA priorities and public guidance.
  - Troubleshot existing detection steps to show how certain TTPs evaded IOC-based detections.
  - Deconflicted events from CISA red team activity, indicating unexpected network/application behavior or the potential presence of a real adversary in the network.

    Note: The team's goal during this phase was to build the organization's ability to detect malicious activity based on adversary behavior (i.e., TTPs) vice relying on known IOCs.

This advisory, drafted in coordination with the assessed organization, details the red team's activity and TTPs, associated network defense activity, and lessons learned to provide network defenders recommendations for improving their organization's defensive cyber posture. The advisory also provides recommendations to software manufacturers to hard their customer networks against malicious activity and reduce the likelihood of domain compromise.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK for Enterprise <https://attack.mitre.org/versions/v15/matrices/enterprise/> framework, version 15. See the MITRE ATT&CK Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK® tactics and techniques. For assistance with mapping malicious cyber

activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping <https://www.cisa.gov/news-events/news/best-practices-mitre-attckr-mapping> and CISA's Decider Tool <https://github.com/cisagov/decider/>.

During the Adversary Emulation phase, the red team gained initial access to the organization's Solaris enclave by exploiting a known vulnerability in an unpatched web server. They gained separate access to the Windows environment by phishing and were able to compromise the full domain and its parent domain. See Figure 1 for a timeline of this assessment and the sections below for details on the team's activity and TTPs.

FIGURE 1: SILENTSHIELD ASSESSMENT TIMELINE

Adversary Emulation Phase

Exploitation of the Solaris Enclave

Reconnaissance, Initial Access, and Command and Control

CISA's red team used open source tools and third-party services to probe the organization's internet-facing surface [T1594 <https://attack.mitre.org/versions/v15/techniques/t1594/>]. This included non-intrusive port scans for common ports and Domain Name System (DNS) enumeration [T1590.002 <https://attack.mitre.org/versions/v15/techniques/t1590/002/>]. These efforts revealed the organization's web server was unpatched for CVE-2022-21587 <https://nvd.nist.gov/vuln/detail/cve-2022-21587>, an unauthenticated remote code execution (RCE) vulnerability in Oracle Web Applications Desktop Integrator. For three months the assessed organization failed to patch this vulnerability, and the team exploited it for initial access.

The exploit provided code execution on a backend application server (SERVER 1) that handled incoming requests from the public-facing web server. The red team used this exploit to upload and run a secure Python remote access tool (RAT). Because the application server had full external internet egress via Transmission Control Protocol (TCP) ports `80` and `443`, the RAT enabled consistent command and control (C2) traffic [T1071.001 <https://attack.mitre.org/versions/v15/techniques/t1071/001/>].

Note: After gaining access, the team promptly informed the organization's trusted agents of the unpatched device, but the organization took over two weeks to apply the available patch. Additionally, the organization did not perform a thorough investigation of the affected servers, which would have turned up IOCs and should have led to a full incident response. About two weeks after the team obtained access, exploit code was released publicly into a popular open source exploitation framework. CISA identified that the vulnerability was exploited by an unknown third party. CISA added this CVE to its Known Exploited Vulnerabilities Catalog <https://www.cisa.gov/known-exploited-vulnerabilities-catalog> on Feb. 2, 2023.

Credential Access, Command and Control, and Privilege Escalation

Once on SERVER 1, the red team probed the host's files and folder structure [T1005 <https://attack.mitre.org/versions/v15/techniques/t1005/>] and identified several old and globally accessible `.tar` backup files, which included a readable copy of an `/etc/shadow` file containing the hash for a privileged service account (ACCOUNT 1). The team quickly cracked the account's weak password using a common wordlist [T1110.002 <https://attack.mitre.org/versions/v15/techniques/t1110/002/>]. They then established an outbound Secure Shell Protocol (SSH) connection over TCP port `80` and used a reverse tunnel to SSH back into SERVER 1, where they were prompted to reset ACCOUNT 1's expired password [T1571 <https://attack.mitre.org/versions/v15/techniques/t1571/>] (see Figure 2). The team identified the account was enabled on a subset of containers, but it had not been actively used in a significant amount of time; the team changed this account's password to a strong password.

FIGURE 2: EXPLOITATION OF THE SOLARIS ENCLAVE

The team discovered ACCOUNT 1 was a local administrator with `sudo/root` access and used it to move laterally (see the next section).

Lateral Movement and Persistence

Servers in the Solaris enclave did not use centralized authentication but had a mostly uniform set of local accounts and permissions [T1078.002 <https://attack.mitre.org/versions/v15/techniques/t1078/002/>]. This allowed the red team to use ACCOUNT 1 to move through much of the network segment via SSH [T1021.004 <https://attack.mitre.org/versions/v15/techniques/t1021/004/>].

Some servers allowed external internet access and the team deployed RATs on a few of these hosts for C2. They deployed several different RATs to diversify network traffic signatures and obfuscate the on-disk and in-memory footprints. These tools communicated to a red team redirector over TCP/`443`, through valid HTTPS messages, and over SSH through non-standard ports (`80` and `443`) [T1571 <https://attack.mitre.org/versions/v15/techniques/t1571/>]. Much of the traffic was not blocked by a firewall, and the organization lacked application layer firewalls capable of detecting protocol mismatches on common ports.

The team then moved laterally to multiple servers, including high value assets, that did not allow internet access. Using reverse SSH tunnels, the team moved into the environment and used a SOCKS proxy [T1090 <https://attack.mitre.org/versions/v15/techniques/t1090/>] to progress forward through the network. They configured implants with TCP bind listeners bound to random high ports to connect directly with some of these hosts without creating new SSH login events (see Figure 3).

FIGURE 3: EXAMPLE OF LATERAL MOVEMENT IN THE SOLARIS ENCLAVE

Once on other internal hosts, the team data mined each for sensitive information and credentials. They obtained personally identifiable information (PII), shadow files, a crackable pass-phrase protected administrator SSH key, and a plaintext password [T1552.003 <https://attack.mitre.org/versions/v15/techniques/t1552/003/>] in a user's `.bash_history`. These data mined credentials provided further avenues for unprivileged access through the network. The team also used SSH tunnels to remotely mount Network File System (NFS) file shares, spoofing `uid` and `gid` values to access all files and folders.

To protect against reboots or other disruptions, the team primarily persisted on hosts usin the `cron` utility [T1053.003 <https://attack.mitre.org/versions/v15/techniques/t1053/003/>], as well as the `at` utility [T1053.002 <https://attack.mitre.org/versions/v15/techniques/t1053/002/>], to run scheduled tasks and blend into the environment. Additionally, SSH private keys provided persistent access to internal pivot hosts and would have continued to enable access even if passwords were rotated.

Full Enclave Compromise

Although ACCOUNT 1 allowed the team to move laterally to much of the Solaris enclave, the account did not provide privileged access to all hosts in the network because a subset of hosts had changed the password (which denied privileged access via that account). However, the team analyzed recent user logins using the `last` command and identified a network security appliance scanning service account (ACCOUNT 2) that logged in regularly to an internal host using password-based authentication. As part of its periodic vulnerability scanning, ACCOUNT 2 would connect to each host via SSH and run `sudo` with a relative path instead of the absolute path `/usr/local/bin/sudo`. The local path created a path hijack vulnerability, which allowed the red team to hijack the execution flow and capture the account's password [T1574.007 <https://attack.mitre.org/versions/v15/techniques/t1574/007/>].

The harvested password granted unrestricted privileged access to the entire Solaris enclave.

Exploitation of the Windows Domain

While the compromise of the Solaris enclave facilitated months of persistent access to sensitive systems, including web applications and databases, it did not lead to the immediate compromise of the corporate Windows environment. Once in the Windows domain, the red team identified several service accounts with weak passwords. It is likely that an adversary could have continued the Solaris attack path through prolonged password spraying attacks, or by leveraging credentials obtained externally (e.g., dark web credential dumps) (see Figure 4).

FIGURE 4: EXPLOITATION OF SOLARIS ENCLAVE

The team exploited the Windows domain through other access vectors and eventually proved the undetected pivot between the domains could be made after they obtained Windows credentials.

Reconnaissance and Initial Access

While attempting to pivot into Windows from Solaris, the red team conducted open source information gathering about the organization. They harvested employee names [T1589.003 <https://attack.mitre.org/versions/v15/techniques/t1589/003/>] and used the information to derive email addresses based on the target's email naming scheme. After identifying names, emails, and job titles, the team selected several phishing targets who regularly interacted with the public [T1591.004 <https://attack.mitre.org/versions/v15/techniques/t1591/004/>]. One user triggered a phishing payload that provided initial access to a workstation.

The team then placed a simple initial access RAT on the workstation in a user-writable folder and obtained user-level persistence through an added registry run key, which called back to a red team redirector via HTTPS. The team assessed what was running on the host in terms of antivirus (AV) and Endpoint Detection and Response (EDR) and used the implant to inject a more capable, full-fledged RAT directly into memory, which pointed to a separate

redirector. The assessed organization's tools failed to categorize C2 traffic as anomalous even when a bug in one of the implants caused 8 GB of continuous network traffic to flow in one afternoon.

Credentialed Access and Privilege Escalation

Internal network information was freely available to unprivileged, domain-joined users, and the team queried hundreds of megabytes of Active Directory (AD) data using a custom rewrite of `dsquery.exe` in `.NET` and Beacon Object File (BOF) `ldapsearch` from the phished user's workstation. The team then data mined numerous internal file servers for accessible shares [T1083 <https://attack.mitre.org/versions/v15/techniques/t1083/>]. The team found a password file left from a previous employee on an open, administrative IT share, which contained plaintext usernames and passwords for several privileged service accounts. With the harvested Lightweight Directory Access Protocol (LDAP) information, the team identified one of the accounts (ACCOUNT 3) had system center operations manager (SCOM) administrator privileges and domain administrator privileges for the parent domain. They identified another account (ACCOUNT 4) that also had administrative permissions for most servers in the domain. The passwords for both accounts had not been updated in over eight years and were not enrolled in the organization's identity management (IDM).

Lateral Movement and Persistence

The team used valid accounts and/or tokens with varied techniques for lateral movement. Techniques included scheduled task manipulation, service creation, and application domain hijacking [T1574.014 <https://attack.mitre.org/versions/v15/techniques/t1574/014/>]. For credential usage, the implemented IDM in the organization's network hampered the red team's ability to pivot as it blocked common credential manipulation techniques like pass-the-hash [T1550.002 <https://attack.mitre.org/versions/v15/techniques/t1550/002/>] and pass-the-ticket [T1550.003 <https://attack.mitre.org/versions/v15/techniques/t1550/003/>]. The red team found ways to circumvent the IDM, including using plaintext passwords to create genuine network logon sessions [T1134.003 <https://attack.mitre.org/versions/v15/techniques/t1134/003/>] for certain

accounts not registered with the IDM, as well as impersonating the tokens of currently logged-in users to piggyback off valid sessions [T1134.001 <https://attack.mitre.org/versions/v15/techniques/t1134/001/>].

The red team tailored payloads to blend with the network's environment and did not reuse IOCs like filenames or file hashes, especially for persisted implants. Remote queries for directory listings, scheduled tasks, services, and running processes provided the information for the red team to masquerade as legitimate activity [T1036.004 <https://attack.mitre.org/versions/v15/techniques/t1036/004/>].

The team emulated normal network activity by installing HTTPS beaconing agents on workstations where normal users browse the web, establishing internal network pivots with TCP bind and SMB listeners. They primarily relied on creating Windows services as their persistence mechanism.

The red team used the data mined credentials for ACCOUNT 3 to move laterally from the workstation to a SCOM server. Once there, using ACCOUNT 4, the team targeted a Systems Center Configurations Manager (SCCM) server, as it was an advantageous network vantage point. The SCCM server had existing logged-in server administrators whose usernames followed a predictable naming pattern (correlating administrative roles and privilege levels), allowing them to determine which account to use to pivot to other hosts.

The team targeted the organization's jump servers frequented by highly privileged administrative accounts. Red team operators used stolen SCCM server administrator credentials to compromise one of the organization's server-administrator jump hosts. They learned that the organization separated some, but not all, accounts onto separate jump servers by role (e.g., workstation administrators and server administrators had separate jump points, but server and domain administrators occasionally shared the same jump hosts). Once a domain administrator logged in, the red team stole the administrator's session token and laterally moved to a domain controller where they pulled credentials for

the entire domain via `DCSync` [T1003.006 <https://attack.mitre.org/versions/v15/techniques/t1003/006/>], obtaining full domain compromise (see Figure 5).

FIGURE 5: EXPLOITATION OF THE WINDOWS DOMAIN

After compromising the domain, the team confirmed access to sensitive servers, including multiple high value assets (HVAs) and tier zero assets. None of the accessed servers had any noticeable additional protections or network access restrictions despite their sensitivity and critical functions in the network. Remote administration and access of these critical systems should be restricted to designated, role-based accounts coming from specific network enclaves and/or workstations. Isolation with these access vector limitations protects them from compromise and sharply reduces the associated noise, allowing defenders to more easily identify abnormal behavior.

Pivoting Into External Trusted Partners

The team inspected the organization's trust relationships with other organizational domains through LDAP [T1482 <https://attack.mitre.org/versions/v15/techniques/t1482/>] and identified connections to multiple external FCEB partner organizations, one of which they subsequently used to move laterally.

The team pulled LDAP information from PARTNER DC 1 and kerberoasted the domain, yielding one valid service account with a weak password they quickly cracked, but the team was unable to move laterally with this account because it lacked appropriate privileges. However, PARTNER 1 had trusted relationships with a second partner's domain controller (PARTNER DC 2). Using the acquired PARTNER 1 credentials, the red team discovered PARTNER 2 also had a kerberoastable, highly privileged administrative service account whose password cracked, allowing the team to laterally move to a PARTNER 2 host from the original victim network (see Figure 6).

FIGURE 6: PATH OF EXPLOITATION INTO EXTERNAL FCEB ORGANIZATIONS

These cross-organizational attack paths are rarely identified or tested in regular assessments or audits due to network ownership, legal agreements, and/or vendor opacity. However, they remain a valuable access vector for advanced persistent threat (APT) actors.

Experimentation with access into trusted partner domains included the modification of local system firewall rules on the source domain controller to allow specific source and destination IPs. The organization's host-based monitoring systems failed to identify the addition and removal of the red team's firewall exceptions.

Defense Evasion Techniques

Solaris Enclave Figure 5: Exploitation of the Windows Domain

Due to the lack of application allowlisting, the red team regularly masqueraded as legitimate software to remain undetected by the organization's network defenders [T1036 <https://attack.mitre.org/versions/v15/techniques/t1036/>]. Additionally, by default, command auditing in Solaris via the `lastcomm` command only captures the program being run—full file path and any command line arguments are not recorded. For example:

- A real file: `/opt/splunkforwarder/bin/splunkd`
- A malicious copy: `/opt/splunkforwarder/splunkd`
- Command auditing logs: `splunkd`

The team also hid common artifacts to obfuscate their operational activity, including modifying file timestamps [T1070.006 <https://attack.mitre.org/versions/v15/techniques/t1070/006/>] and permissions with the `touch` and `chmod/chown` commands [T1222.002 <https://attack.mitre.org/versions/v15/techniques/t1222/002/>] to blend with other files in the environment.

Windows Domain

The team used a diverse range of accounts, backdoors, and C2 channels with different network footprints to obfuscate activity [T1027 <https://attack.mitre.org/versions/v15/techniques/t1027/>].

Diversification of account usage, backdoors, and C2 channels further obfuscated red team activity in the domain. Lateral movement to new hosts featured a variety of accounts to reduce the risk of detection. When harvesting credentials, the team selected several backup accounts for each role (e.g., server admin, workstation admin, domain admin, service accounts) in case the intended account was locked, disabled, or flagged as compromised.

To emphasize the value of tool-agnostic/behavior-based detections, the red team deployed over seven different implants to mimic real-world adversaries' diverse use of open source, commercial off-the-shelf (COTS), and custom RATs. Each featured different host and network signatures to evade out-of-the-box EDR detections and every implant had unique artifacts both on-disk and in-memory. The team also evaded EDR/AV by using proprietary loaders and beacon object files (BOFs) to make direct API calls and allow self-injection of `.NET` executables to run additional capabilities.

All the deployed tools had different network C2 channel footprints. Some beaconing agents connected via HTTPS to legitimate domains owned by the red team. Others used domain fronting [T1090.004 <https://attack.mitre.org/versions/v15/techniques/t1090/004/>] to leverage common content delivery network (CDN) functionality. Outbound traffic sent to public websites not owned by the red team had a `Host` header that told the CDN provider it should redirect traffic to red-team-controlled IP addresses. Internal pivots used SMB on port `445` and TCP bind listeners on ephemeral high ports. The team tailored both to mim named pipes and network connections already seen in the domain and evade detection.

Collaborative Phase

Five months into the assessment, the red team officially notified the organization's security operations center (SOC) of the ongoing activity and began engaging directly with SOC leadership. At this point, the organization had not submitted deconflictions and did not appear to be actively investigating CISA SILENTSHIELD assessment activity.

During this phase, CISA refrained from providing TTPs or IOCs (such as concrete hosts, filenames, or C2 domains) to allow the organization to develop and test its own detection metrics. The team held weekly discussions with the organization's senior technical staff, SOC, and system administrators, which led to measurable improvements in response times for known techniques and behavior-based detections that uncovered previously unknown tradecraft. Specifically, the red team worked with the organization to assist them with synthesizing the following data sources to identify the extent of the red team's compromise:

- EDR alerts;
- YARA scans;
- C2 domains and techniques;
- Internal pivot hosts;
- Admin accounts used to pivot;
- Memory dumps, revealing attempts to pass credentials; and
- Email logs documenting the initial breach via phishing.

Every cyber threat actor has a unique set of TTPs. Nevertheless, nearly all adversaries perform the same basic steps:

- Command execution (initial access and lateral movement);
- Establish C2 channels and exfiltrate data;
- Establish persistence;
- Escalate privileges; and
- Use and abuse credentials.

All TTPs have corresponding artifacts, but not all IOCs are created equal. Fixating on a hyper-focused set of IOCs can catch known threats but impedes efforts to identify unknown adversaries employing different TTPs.

Major themes discussed during this phase that improved the organization's behavior-based detection capabilities included log collection, forensic analysis, relying on IOCs for detection, monitoring and investigation management, and Sysmon misconfigurations.

Log Collection

The assessed organizations had ineffective and insufficient logs, and network defenders were not using logs to proactively detect anomalous behavior. With the red team's assistance, the organization identified logging issues caused by hardware failures, limited backups, network bandwidth, and limited log collection and retention policies (only 60–90 days). In other cases, critical data was captured but not analyzed because artifacts were moved to cold storage.

The organization's network defenders identified procedural and other roadblocks when attempting to acquire new forensic data. For example, affected servers could not be taken offline for imaging because there was no process in place to do so without impacting the organization's operations. Additionally, attempts to capture forensic data via packet captures occurred directly on the compromised Solaris and Windows hosts, where the red team observed the data being collected and therefore had the opportunity to disrupt collection, tamper with evidence files, and better adapt and evade their defenses.

Forensic Analysis

Defenders did not monitor C2 egress via DNS. They believed their parent entity was monitoring their DNS traffic, absolving them of a need to collect and monitor logs for their analyses.

Forensic analysts blindly trusted the timestamps for files and persistence mechanisms without realizing they had been tampered with. Bogus times added to persistence mechanisms (such as scheduled tasks) led defenders to misjudge the timeline of the breach. Red team operators regularly adjusted the last-modified timestamp of files and folders—using either the native `touch -r` command or implants' `timestomp` command to disguise the last-modified timestamp captured in the output of `ls –la`.

Secondary file timestamps identified with `ls -lu` or `ls -lc` would have revealed abnormal file attributes, in addition to more reliable anomalies found during proper forensic investigation.

Reliance on Known IOCs

The red team used diversified TTPs in the Adversary Emulation phase to reflect the ability of cyber threat actors to bypass conventional, known-bad detection strategies. The network defenders did not detect much of the team's activity. For example:

- After identifying a red team payload, network defenders wrote tailored YARA rules that signatured specific behavior of the red team's loader, which uncovered several similar payloads but failed to catch any of the other six C2 frameworks.
- Organization network defenders used a combination of custom and open source detection rules (such as `CommandLine=kerberoast*` or files called `bloodhound.zip`) and did not detect the team's kerberoasting activity.

Regular Monitoring and Investigation Management

Conversations with SOC leadership revealed several procedural issues that led to slow or incomplete analysis of the red team's intrusion and activity. For example:

- While EDR products detected and quarantined several of the red team's tools, including the initial phishing payload, the organization's daily procedures did not always include review of EDR alerts. The red team worked with the organization to ensure rapid response to EDR alerts became a fundamental part of network defenders' daily workflows. This allowed SOC personnel to identify new attempts at lateral movement.
- Solaris network owners discovered that several firewalls had inadvertently been misconfigured or disabled. The organization's technical teams worked directly with the red team to fix errors and to reorganize and revalidate the network topology.

- Network defenders had poor operational security and alerted the red team of investigations. For example:
  - In one instance, after receiving incoming beacons from what was evidently a sandboxed environment, the payload was not renamed from its original file, allowing the red team to immediately identify how much of their access was under scrutiny. Organizations must ensure sandboxed environments are safe, secure, and thoroughly sandboxed.
  - The red team observed system administrators reviewing forensic artifacts tied to the team's Solaris payload—searching for files, running packet captures for outbound C2 traffic, and port scanning the C2 redirector. Team members simply reinstalled their persistence with a new redirector and file path, sidestepping the informal investigation.
- IT teams were siloed from the SOC, who had no knowledge of the system administrator's weeks long investigation into the anomalous network behavior.
- While the organization compartmented most of its threat hunting and incident response in a separate domain, staff still used the compromised corporate domain accounts to communicate the details of active investigations and assessments.

Sysmon Misconfigurations

The red team had a productive exchange with the organization on their Sysmon configuration, which the team abused throughout the assessment. The red team identifie several misconfigurations:

- Deployment teams pushed the ruleset (stored as a `.xml` file) to a globally readable `C:\Windows` directory. There were no rules in place to catch adversaries reading the configurations from disk or the registry. As a result, CISA's red team was provided explicit file paths to safely place their payloads.
- Rules targeted a single, tool-specific IOC rather than a technique (e.g., `sc.exe` rather than service creation events).
- Exceptions were overly permissive (for example, excluding all Image entries anywhere in `C:\Program Files (x86)\Google\Update\*`).

LESSONS LEARNED AND KEY FINDINGS

The red team noted the following lessons learned and key findings relevant to the security of the assessed organization's network. These specific findings contributed to the team's ability to gain persistent access across the organization's network. See the Mitigations section for recommendations on how to address these findings.

Lesson Learned: The assessed organization had insufficient controls to prevent and detect malicious activity.

- **Finding #1: The organization's perimeter network was not adequately firewalled from its internal network, which failed to restrict outbound traffic.** A majority of the organization's hosts, including domain controllers, had internet connectivity to broad AWS EC2 ranges, allowing the red team to make outbound web requests without triggering IDS/IPS responses. These successful connections revealed the lack of an application layer firewall capable of detecting protocol mismatches on common ports.
- **Finding #2: The assessed organization had insufficient network segmentation.** The lack of network segmentation allowed the red team to move into, within, and out of both the Solaris and Windows domain. This also enabled them to gather a massive amount of data about the organization and its systems. Internal servers could reach almost any other domain host, regardless of type (server vs. workstation), purpose (us laptop, file server, IDM server, etc.), or physical location. Use of network address translation (NAT) between different parts of the network further obfuscated data streams, hindering incident response.
- **Finding #3: The organization had trust relationships with multiple partner organizations,** which—when combined with weak credentials and network connectivity—allowed the red team to exploit and move laterally to a partner domain controller. This highlights the risk of blindly allowing third party network connectivity and the importance of regularly monitoring both privileged access and transitive trusted credential material**.**

- **Finding #4: The organization's defensive staff did not sufficiently isolate their defensive investigative activity.** Organizations should always communicate information pertaining to suspected incidents out-of-band, rather than from within a domain that they know to be compromised. While the defensive systems were shunted to another domain with correct (one-way) trusts, the red team identified a likely attack vector to that domain via the same, previously compromised IDM server. Some analysts also performed dynamic analysis of suspected implants from an internet-connected sandbox, tipping the red team to the specific files and hosts that were under investigation.
- **Finding #5: Network defenders were not familiar with the intricacies of their IDM solution.** The CISA red team identified accounts not enrolled in the IDM and successfully used those and already existing user access tokens to bypass IDM. The appliance, in its active configuration, was not exhaustively tested against common credential manipulation techniques nor were any alerts on anomalous behavior being monitored.
- **Finding #6: The organization had some role-based host segmentation, but it was not granular enough.** The organization used clearly defined roles (server administrator and domain administrator) but did not sufficiently segregate the accounts to their own servers or systems, enabling privilege escalation.

Lesson Learned: The organization did not effectively or efficiently collect, retain, and analyze logs.

- **Finding #7**: **Defensive analysts did not have the information they needed** due to a combination of issues with collecting, storing, and processing logs. Other policies collected too much useless data, generating noise and slowing investigation.
- **Finding #8: Network defenders' daily procedures did not always include analysis of EDR alerts**, and the tools that were installed only provided a 30-day retention for quarantined files. Consequently, investigators were unable to access timely information that may have led to earlier detection of the red team's activity.
- **Finding #9: Forensic analysts trusted host artifacts that could have been modified by an adversary.** In particular, file timestamps and packet captures were scrutinized without considering the possibility of malicious tampering.

Lesson Learned: Bureaucratic communication and decentralized teams hindered the organization's network defenders.

- **Finding #10: The organization's technical staff were spread across decentralized teams.** Siloed team structure meant that IT, security, and other technical teams lacked consistency with their tools, creating too much noise for defenders to sift through.
- **Finding #11: The SOC team lacked the agency to rapidly update or deploy rulesets through the fractured IT teams**. The organization diffused responsibility for individual tools, such as Sysmon, across multiple groups, hampering timeliness and maintenance of a defensive posture.
- **Finding #12**: **The organization's forensics team produced an incident response report which documented the red team's initial exploitation of the Solaris enclave. However, the report was limited in scope and did not adequately document the red team's ability to expand and persist**. The success of the red team's first phase, using publicly known TTPs, illustrated the business risk to all Solaris hosts and, by extension, the Windows environment. Moreover, the organization's internal report only focused on vulnerable servers and did not account for a cyber threat actor's ability to expand and persist in the Solaris enclave.
  - The Solaris administrator's investigations of the red team failed to appear in either the report or in SOC deconflictions. An admin's inquiry into unusual and probably malicious activity, particularly in the middle of an investigation of confirmed breaches of adjacent hosts, should have been considered in the report as evidence of lateral movement.

Lesson Learned: A "known-bad" detection approach hampered detection of alternate TTPs.

- **Finding #13**: **Defenders hyper-focused on specific IOCs, such as file attributes, particular C2 frameworks, or C2 domains.** The organization's network defenders did not initially employ tool-agnostic detections, causing them to positively identify some red team tools, but remain blind to the full extent of the compromise. They were accustomed to catching internal red teams that used specific TTPs; introducing a new "threat actor" with new TTPs sidestepped nearly all detections.

- **Finding #14**: **Detection rules were visible from compromised systems**, allowing the red team to sidestep detections based on hardcoded rules and exceptions.
- **Finding #15: There was insufficient restriction of administrative tools.** The technical staff lacked a standardized set of administrative tools, leaving all remote administration protocols available for use by admins, CISA red team, or adversaries. This also created excessive noise for defenders to effectively sift through to determine expected versus anomalous activity.
- **Finding #16: There was insufficient tracking of software**. There was no apparent approval or tracking process for software installation across the domain, preventing defensive analysts from identifying abnormal software placed by the red team. A comprehensive inventory of approved software would help defenders identify abnormal behavior and facilitate the deployment of application allow-listing.

NOTED STRENGTHS

The assessed organization promptly planned for and resolved multiple identified issues, including with:

- **Windows service accounts**: The organization eliminated over 30 percent of service accounts which were deemed unnecessary. There is an on-going effort to change service account passwords and apply DoD recommended STIG compliance (over 85 percent have been changed since the publication of this report).
- **IDM**: The organization is looking into how to improve their IDM implementation and apply additional security alerts and preventions for possible misuse of credentials. They plan to implement additional identity-based monitoring capabilities in front of tier zero assets.
- **Egress**: The organization implemented new processes to detect and prevent servers from anomalously egressing outside of the network to the internet.
- **Host-based solutions**: The organization used additional features of their antivirus software, such as reputation scores, to look for all executable file type outliers of to identify anomalous instances.
- **Hosts**: The organization decommissioned clusters of servers and completely rebuilt them from scratch after identifying numerous irreparable issues and misconfigurations.

- **Solaris credentials**: The organization changed passwords, removed SSH keys, restricted permissions, and removed unnecessary accounts.

MITIGATIONS

Network Defenders

CISA recommends organizations implement the recommendations in Table 1 to mitigate the findings listed in the Lessons Learned and Key Findings section of this advisory. 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. See CISA's Cross-Sector Cybersecurity Performance Goals <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals> for more information on the CPGs, including additional recommended baseline protections.

Table 1: Recommendations to Mitigate Identified Issues

Finding	Recommendation

Finding	Recommendation
Inadequate firewall between perimeter and internal devices	■ Deploy internal and external network firewalls to inspect, log, and/or block unknown or unauthorized traffic. ■ Perform deep packet inspection to detect mismatched application traffic or encrypted data flows. ■ Restrict outbound internet egress to hosts whenever possible. ■ Establish a baseline of normal user activity, including unique IPs or domains.

Finding	Recommendation
Insufficient Network Segmentation	■ Apply the principle of least privilege to limit the exposure of systems and services in the demilitarized zone (DMZ). ■ Segment the DMZ based on the sensitivity of systems and services as well as the internal network [CPG 2.F <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#networksegmentation2f>]. ■ Segment networks to protect assets and workstations from direct exposure to the internet by considering the criticality of the asset to business functions, sensitivity of the data traversing the asset, and requirements for internet access to the asset. ■ Implement and regularly test firewalls, access control lists, and intrusion prevention systems. ■ Take advantage of opportunities to create natural network segmentation. Securely configured VPNs used for remote laptops, for instance, create an easy place to filter and monitor incoming traffic.

Finding	Recommendation
Trust relationships between domains were overly permissive	■ Restrict network connectivity (ingress and egress) to only necessary services between trusted domains [CPG 2.E <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#separatinguserandprivilegedaccounts2e>]. ■ Regularly monitor privileged access via Foreign Security Principals (FSPs).
Defensive activity was not sufficiently isolated	■ Perform network defense investigations out-of-band [CPG 3.A <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#detectingrelevantthreatsandttps3a>]. ■ Conduct regular security audits and penetration testing by internal and external parties. ■ Develop and implement a comprehensive Incident Response Plan (IRP) and conduct regular drills and simulations [CPG 2.S <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#incidentresponseirplans2s>].

Finding	Recommendation
IDM solutions were not fully understood and utilized	■ Enroll all accounts in IDM solutions and test against common credential manipulation techniques. ■ Integrate the IDM solution with other systems and applications, allowing for the streamlining of workflows.
Insufficient role-based host segmentation	■ Establish Role-Based Access Controls (RBAC) to systematically assign permissions based on job functions [CPG 2.E <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#separatinguserandprivilegedaccounts2e>]. ■ Implement a comprehensive security model incorporating micro-segmentation at the host level.

Finding	Recommendation
Failure to monitor EDR alerts daily	■ Develop and document Standard Operating Procedures (SOPs) for handling EDR alerts [CPG 5.A <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#incidentplanningandpreparedness5a>]. ■ Establish and maintain incident response playbooks. ■ Conduct regular audits and reviews of the EDR alert handling process.
Host artifacts were overly trusted	■ Operationalize and deploy File Integrity Monitoring (FIM) solutions. ■ Regularly review and adjust access permissions, adhering to the principle of least privilege [CPG 2.E <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#separatinguserandprivilegedaccounts2e>]. ■ Establish proper forensic processes to ensure integrity.

Finding	Recommendation
Bureaucracy and decentralization of network defenders hampered communication and consistency	■ Introduce cross-training initiatives to cultivate a collaborative culture. ■ Encourage the establishment of cross-functional projects. ■ Utilize collaboration platforms that seamlessly integrate various tools and systems.
Insufficient internal incident response report	■ Promote a culture of ongoing improvement while also fostering a proactive approach among employees to promptly report suspicious activities. ■ Treat suspected incidents of compromise as a confirmed breach, and account for a threat actor's ability to move laterally when defining the scope of incident response efforts.

Finding	Recommendation
Focus on known/common IOCs	■ Employ centralized logging and tool-agnostic detection methods. ■ Leverage threat intelligence feeds by integrating them into a SIEM tool. ■ Implement regular updates for IOCs and TTPs, with the capability for customization to address the specific threat landscape [CPG 3.A <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#detectingrelevantthreatsandttps3a>].
Detection rules were visible from compromised systems	■ Integrate runtime detection mechanisms while removing world-readable configuration files from installer deployments where applicable.

Finding	Recommendation
Insufficient restriction of admin tools	■ Enhance security posture by implementing application allowlisting to ensure only trusted and approved applications are permitted [CPG 2.Q <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#hardwareandsoftwareapprovalprocess2q>]. ■ Apply the principle of least privilege by granting users only the minimum level of access necessary to perform job functions.
Insufficient tracking of software	■ Conduct a comprehensive inventory of assets and establish a baseline for behavior [CPG 1.A <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#assetinventory1a>]. ■ Utilize a Software Asset Management (SAM) solution that offers comprehensive tracking, reporting, and compliance management capabilities. ■ Deploy automated discovery and monitoring tools to continuously scan and identify new and existing software.

CISA recommends organizations implement the recommendations in Table 2 to mitigate other identified issues that can be uncovered through traditional penetration tests or red team assessments.

Table 2: Recommendations to Mitigate Identified Issues

Issue	Recommendation
Accounts were overprivileged and the organization's network contained unnecessary service accounts	■ Apply the principle of least privilege when assigning permissions to user accounts. Audit existing group memberships, strip unnecessary privileges, and prune unnecessary nested groups/users. ■ Monitor for account lockout, especially on administrative accounts, and switch to a manual account unlock policy. ■ Increase monitoring for higher-risk accounts, such as service accounts, that are highly privileged and have a predictable pattern of behavior (e.g., scans that reliably run at a certain hour of the day). ■ Privileged users should have dedicated role-based user accounts and associated jump hosts to log into critical resources.

Issue	Recommendation
Insufficient EDR configuration	■ Ensure all hosts have a form of EDR installed. ■ Deploy an EDR capable of catching commonly known obfuscation or execution techniques.
Insecure and insufficient credentials	■ Ensure sensitive credentials and documents are not stored in an accessible place. ■ Mandate strong and complex passwords [CPG 2.B <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#minimumpasswordstrength2b>]. For more information, see CISA's Secure Our World: Require Strong Passwords. <https://www.cisa.gov/secure-our-world/require-strong-passwords>

Note: The above mitigations apply to critical infrastructure organizations with on-premises or hybrid environments. CISA encourage all organizations to **prioritize purchasing products from manufacturers who demonstrate secure by design principles**, such as evidenced by follow-on publications from companies who have signed the Secure by Design Pledge <https://www.cisa.gov/securebydesign/pledge>.

Software Manufacturers

CISA recognizes that insecure software is the root cause of many flaws; the responsibility should not rest on the end user. CISA urges software manufacturers to implement the following:

- **Eliminate default passwords** <https://www.cisa.gov/resources-tools/resources/secure-design-alert-how-manufacturers-can-protect-customers-eliminating-default-passwords> and determine what password practices should be required (such as minimum password length and disallowing known breached passwords). Configure software to use more secure authentication schemes by default.
- **Provide logging at no additional charge**. Cloud services and on-premises products should commit to generating and storing security related logs at no additional cost.
- **Work with security information and event management (SIEM) and security orchestration, automation, and response (SOAR) providers**—in conjunction with customers—to understand how response teams use logs to investigate incidents. The goal is to develop logs that yield a comprehensive story of the event.
- **Remove unnecessary software dependencies**. Unnecessary software increases the attack surface available to adversaries and may introduce additional vulnerabilities. Mitigating these additional vulnerabilities requires significant investment, consuming resources like time, technical personnel, and adding to the level of security effort.

These mitigations align with tactics provided in the joint guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software <https://www.cisa.gov/sites/default/files/2023-10/shifting-the-balance-of-cybersecurity-risk-principles-and-approaches-for-secure-by-design-software.pdf>. CISA urges software manufacturers to take ownership of improving the security outcomes of their customers by applying these and other secure by design tactics. By using secure by design tactics, software manufacturers can make their product lines secure “out of the box” without requiring customers to spend additional resources making configuration changes, purchasing security software and logs, monitoring, and making routine updates.

For more information on secure by design, see CISA's Secure by Design <https://www.cisa.gov/securebydesign> webpage. For more information on common misconfigurations and guidance on reducing their prevalence, see joint advisory NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a>.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, CISA recommends exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. CISA recommends testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Tables 3–11).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

CISA recommends continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

RESOURCES

- Layering Network Security Through Segmentation <https://www.cisa.gov/resources-tools/resources/layering-network-security-through-segmentation-infographic>

- Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies <https://www.cisa.gov/resources-tools/resources/ics-recommended-practices>
- Phishing Guidance: Stopping the Attack Cycle at Phase One <https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one>
- BOFs <https://hstechdocs.helpsystems.com/manuals/cobaltstrike/current/userguide/content/topics/beacon-object-files_main.htm>
- Detecting DCSync <https://blog.blacklanternsecurity.com/p/detecting-dcsync>
- App Domain Hijacking Overview <https://pentestlaboratories.com/2020/05/26/appdomainmanager-injection-and-detection/>

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. CISA does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation or favoring by CISA.

VERSION HISTORY

July 11, 2024: Initial version.

APPENDIX: MITRE ATT&CK TACTICS AND TECHNIQUES

See Tables 3–11 for all referenced threat actor tactics and techniques in this advisory.

Table 3: Reconnaissance

Technique Title	ID	Use

Technique Title	ID	Use
Search Victim-Owned Websites	T1594 <https://attack.mitre.org/versions/v15/techniques/t1594/>	CISA's red team used open source tools and services to probe the organization's internet-facing presence and gather information, including names, roles, and contact information.
Gather Victim Network Information: DNS	T1590.002 <https://attack.mitre.org/versions/v15/techniques/t1590/002/>	The red team gathered information about the organization's DNS records, which revealed several details about the organization's internal network.
Gather Victim Identity Information: Employee Names	T1589.003 <https://attack.mitre.org/versions/v15/techniques/t1589/003/>	CISA's red team collected the assessed organizations' employee names to use their email addresses for specific targeting based on roles and responsibilities.

Technique Title	ID	Use
Gather Victim Org Information: Identity Roles	T1591.004 <https://attack.mitre.org/versions/v15/techniques/t1591/004/>	CISA's red team selected specific individuals from the assessed organization and targeted them with phishing payloads.

Table 4: Command and Control

Technique Title	ID	Use
Application Layer Protocol: Web Protocols	T1071.001 <https://attack.mitre.org/techniques/t1071/001/>	The red team exploited CVE-2022-21587 <https://nvd.nist.gov/vuln/detail/cve-2022-21587> and ran a RAT that provided consistent C2 via open Transmission Control Protocol (TCP) ports.
Non-Standard Port	T1571 <https://attack.mitre.org/versions/v15/techniques/t1571/>	The red team used SSH over ports `80` and/or `443` when establishing outbound C2.
Proxy: Domain Fronting	T1090.004 <https://attack.mitre.org/versions/v15/techniques/t1090/004/>	CISA's red team leveraged domain fronting to redirect and obfuscate their traffic.

Table 5: Credential Access

Technique Title	ID	Use
Brute Force: Password Cracking	T1110.002 <https://attack.mitre.org/versions/v15/techniques/t1110/002/>	The red team cracked an account's password by using a common wordlist.
OS Credential Dumping: DCSync	T1003.006 <https://attack.mitre.org/versions/v15/techniques/t1003/006/>	CISA's red team pulled credentials for the domain via DCSync to gain full access to the domain.
Unsecured Credentials: Bash History	T1552.003 <https://attack.mitre.org/versions/v15/techniques/t1552/003/>	The red team obtained a password by searching a user's bash command history, which provided further unprivileged access throughout the network.

Table 6: Discovery

Technique Title	ID	Use

Technique Title	ID	Use
Domain Trust Discovery	T1482 <https://attack.mitre.org/versions/v15/techniques/t1482/>	CISA's red team inspected the assessed organization's domain trust relationships through LDAP and identified potential connections in external organizations to which to move laterally.
File and Directory Discovery	T1083 <https://attack.mitre.org/versions/v15/techniques/t1083/>	The red team data mined numerous internal servers and discovered one misconfigured share that contained plaintext usernames and passwords for several privileged service accounts.

Give Feedback

Table 7: Privilege Escalation

Technique Title	ID	Use

Technique Title	ID	Use
Hijack Execution Flow: Path Interception by PATH Environment Variable	T1574.007 <https://attack.mitre.org/versions/v14/techniques/t1574/007/>	The red team hijacked the execution flow of a program that used a relative path instead of an absolute path, which enabled the capture of the account's password.
Access Token Manipulation: Token Impersonation/Theft	T1134.001 <https://attack.mitre.org/versions/v15/techniques/t1134/001/>	CISA's red team impersonated the tokens of current users to exploit valid sessions and bypass the organization's IDM.
Access Token Manipulation: Make and Impersonate Token	T1134.003 <https://attack.mitre.org/versions/v15/techniques/t1134/003/>	CISA's red team created new tokens and logon sessions for accounts not registered with the IDM to escalate privileges.

Table 8: Lateral Movement

Technique Title	ID	Use
Remote Services: SSH	T1021.004 <https://attack.mitre.org/versions/v15/techniques/t1021/004/>	CISA's red team used SSH with a valid account to move through the enclave.

Technique Title	ID	Use
Proxy	T1090 <https://attack.mitre.org/versions/v15/techniques/t1090/>	The red team used a SOCKS proxy to avoid direct connections to their infrastructure and obscure the source of the malicious traffic.
Use Alternate Authentication Material: Pass the Hash	T1550.002 <https://attack.mitre.org/techniques/t1550/002/>	The red team's operations were hindered by the organization's IDM when it blocked the team's attempts to bypass system access controls using different hash types for authentication.
Use Alternate Authentication Material: Pass the Ticket	T1550.003 <https://attack.mitre.org/versions/v15/techniques/t1550/003/>	CISA's red team's operations were hindered by the organization's IDM when it blocked the team's attempts to bypass system access controls using Kerberos tickets for authentication.

Table 9: Collection

Technique Title	ID	Use

Technique Title	ID	Use
Data from Local System	T1005 <https://attack.mitre.org/versions/v15/techniques/t1005/>	CISA's red team searched each host for files containing sensitive or interesting information such as password hashes, account information, network configurations, etc.

Table 10: Persistence

Technique Title	ID	Use
Scheduled Task/Job: Cron	T1053.003 <https://attack.mitre.org/versions/v15/techniques/t1053/003/>	The red team used the `cron` utility to perform task scheduling and execute malicious code within Unix systems at specified times.
Scheduled Task/Job: At	T1053.002 <https://attack.mitre.org/versions/v15/techniques/t1053/002/>	CISA's red team used the `at` utility to perform task scheduling and execute malicious code within Unix systems at a specified time and date.

Technique Title	ID	Use
Hijack Execution Flow: AppDomainManager	T1574.014 <https://attack.mitre.org/versions/v15/techniques/t1574/014/>	The red team executed malicious payloads by hijacking how the `.NETAppDomainManager` loads assemblies.
Valid Accounts: Domain Accounts	T1078.002 <https://attack.mitre.org/versions/v15/techniques/t1078/002/>	CISA's red team regularly used compromised valid domain accounts managed by Active Directory, giving access to resources of the domain.

Table 11: Defensive Evasion

Technique Title	ID	Use
Masquerading: Masquerade Task or Service	T1036.004 <https://attack.mitre.org/versions/v15/techniques/t1036/004/>	The red team enumerated local files and running processes to gather information for their payloads and persistence mechanisms to appear as legitimate activity.

Technique Title	ID	Use
Obfuscated Files or Information	T1027 <https://attack.mitre.org/versions/v15/techniques/t1027/>	CISA's red team encrypted, encoded, and obfuscated their executables and C2 channels to evade defenses across the network.
File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification	T1222.002 <https://attack.mitre.org/versions/v15/techniques/t1222/002/>	The red team modified file permissions with `touch` and `chmod/chown` commands to obfuscate their activity and blend in with other files in the environment.
Indicator Removal: Timestomp	T1070.006 <https://attack.mitre.org/versions/v15/techniques/t1070/006/>	CISA's red team modified file timestamps to hide their operational activity.

Tags

MITRE ATT&CK TTP: Collection (TA0009), Command and Control (TA0011), Credential Access (TA0006), Defense Evasion (TA0005), Discovery (TA0007), Lateral

Movement (TA0008), Persistence (TA0003), Privilege Escalation (TA0004), Reconnaissance (TA0043)

Topics: Critical Infrastructure Security and Resilience </topics/critical-infrastructure-security-and-resilience>, Cyber Threats and Advisories </topics/cyber-threats-and-advisories>, Cybersecurity Best Practices </topics/cybersecurity-best-practices>, Incident Detection, Response, and Prevention </topics/cyber-threats-and-advisories/incident-detection-response-and-prevention>

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Give Feedback

Related Advisories

SEP 23, 2025 ■ CYBERSECURITY ADVISORY | AA25-266A

CISA Shares Lessons Learned from an Incident Response Engagement </news-events/cybersecurity-advisories/aa25-266a>

AUG 27, 2025 ■ CYBERSECURITY ADVISORY | AA25-239A

Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System </news-events/cybersecurity-advisories/aa25-239a>

JUL 31, 2025 ■ CYBERSECURITY ADVISORY | AA25-212A

CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt at US Critical Infrastructure Organization

</news-events/cybersecurity-advisories/aa25-212a>

JUL 22, 2025 ■ CYBERSECURITY ADVISORY | AA25-203A

#StopRansomware: Interlock

</news-events/cybersecurity-advisories/aa25-203a>

Return to top

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov