Recommended steps

Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization | CISA

DETECTION

Given the actors' demonstrated capability to maintain persistent, long-term access in compromised enterprise environments, CISA, FBI, and NSA encourage organizations to:

- **Monitor logs for connections from unusual VPSs and VPNs.** Examine connection logs for access from unexpected ranges, particularly from machines hosted by SurfShark and M247.
- **Monitor for suspicious account use** (e.g., inappropriate or unauthorized use of administrator accounts, service accounts, or third-party accounts). To detect use of compromised credentials in combination with a VPS, follow the steps below:
    - **Review logs for "impossible logins,"** such as logins with changing username, user agent strings, and IP address combinations or logins where IP addresses do not align to the expected user's geographic location.
    - **Search for "impossible travel,"** which occurs when a user logs in from multiple IP addresses that are a significant geographic distance apart (i.e., a person could not realistically travel between the geographic locations of the two IP addresses in the time between logins). **Note:** This detection opportunity can result in false positives if legitimate users apply VPN solutions before connecting to networks.
    - **Search for one IP used across multiple accounts**, excluding expected logins.
        - Take note of any M247-associated IP addresses used along with VPN providers (e.g., SurfShark). Look for successful remote logins (e.g., VPN, OWA) for IPs coming from M247- or using SurfShark-registered IP addresses.
    - **Identify suspicious privileged account use** after resetting passwords or applying user account mitigations.
    - **Search for unusual activity in typically dormant accounts.**
    - **Search for unusual user agent strings,** such as strings not typically associated with normal user activity, which may indicate bot activity.
- **Review the YARA rules provided in MAR-10365227-1** to assist in determining whether malicious activity has been observed.
- **Monitor for the installation of unauthorized software,** including Remote Server Administration Tools (e.g., psexec, RdClient, VNC, and ScreenConnect).

- **Monitor for anomalous and known malicious command-line use.** See Appendix: Windows Command Shell Activity for commands used by the actors to interact with the victim's environment.
- **Monitor for unauthorized changes to user accounts** (e.g., creation, permission changes, and enabling a previously disabled account).

CONTAINMENT AND REMEDIATION

Organizations affected by active or recently active threat actors in their environment can take the following initial steps to aid in eviction efforts and prevent re-entry:

- **Report the incident.** Report the incident to U.S. Government authorities and follow your organization's incident response plan.
    - Report incidents to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870).
    - Report incidents to your local FBI field office at fbi.gov/contact-us/field-offices or to FBI's 24/7 Cyber Watch (CyWatch) via (855) 292-3937 or CyWatch@fbi.gov.
    - For DIB incident reporting, contact the Defense Cyber Crime Center (DC3) via DIBNET at dibnet.dod.mil/portal/intranet or (410) 981 0104.
- **Reset all login accounts.** Reset all accounts used for authentication since it is possible that the threat actors have additional stolen credentials. Password resets should also include accounts outside of Microsoft Active Directory, such as network infrastructure devices and other non-domain joined devices (e.g., IoT devices).
- **Monitor SIEM logs and build detections.** Create signatures based on the threat actor TTPs and use these signatures to monitor security logs for any signs of threat actor re-entry.
- **Enforce MFA on all user accounts.** Enforce phishing-resistant MFA on all accounts without exception to the greatest extent possible.
- **Follow Microsoft's security guidance for Active Directory**—Best Practices for Securing Active Directory.
- **Audit accounts and permissions.** Audit all accounts to ensure all unused accounts are disabled or removed and active accounts do not have excessive privileges. Monitor SIEM logs for any changes to accounts, such as permission changes or enabling a previously disabled account, as this might indicate a threat actor using these accounts.
- **Harden and monitor PowerShell** by reviewing guidance in the joint Cybersecurity Information Sheet—Keeping PowerShell: Security Measures to Use and Embrace.

Mitigations

Mitigation recommendations are usually longer-term efforts that take place before a compromise as part of risk management efforts, or after the threat actors have been evicted from the environment and the immediate response actions are complete. While some may be tailored to the TTPs used by the threat actor, recovery recommendations are largely general best practices and industry standards aimed at bolstering overall cybersecurity posture.

Segment Networks Based on Function

- **Implement network segmentation to separate network segments based on role and functionality**. Proper network segmentation significantly reduces the ability for ransomware and other threat actor lateral movement by controlling traffic flows between—and access to—various subnetworks. (See CISA's Infographic on Layering Network Security Through Segmentation and NSA's Segment Networks and Deploy Application-Aware Defenses.)
- **Isolate similar systems and implement micro-segmentation with granular access and policy restrictions** to modernize cybersecurity and adopt Zero Trust (ZT) principles for both network perimeter and internal devices. Logical and physical segmentation are critical to limiting and preventing lateral movement, privilege escalation, and exfiltration.

Manage Vulnerabilities and Configurations

- **Update software**, **including operating systems**, **applications**, **and firmware**, **on network assets**. Prioritize patching known exploited vulnerabilities and critical and high vulnerabilities that allow for remote code execution or denial-of-service on internet-facing equipment.
- **Implement a configuration change control process** that securely creates device configuration backups to detect unauthorized modifications. When a configuration change is needed, document the change, and include the authorization, purpose, and mission justification. Periodically verify that modifications have not been applied by comparing current device configurations with the most recent backups. If suspicious changes are observed, verify the change was authorized.

Search for Anomalous Behavior

- **Use cybersecurity visibility and analytics tools** to improve detection of anomalous behavior and enable dynamic changes to policy and other response actions. Visibility tools include network monitoring tools and host-based logs and monitoring tools, such as an endpoint detection and response (EDR) tool. EDR tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- **Monitor the use of scripting languages** (e.g., Python, Powershell) by authorized and unauthorized users. Anomalous use by either group may be indicative of malicious activity, intentional or otherwise.

Restrict and Secure Use of Remote Admin Tools

- **Limit the number of remote access tools as well as who and what can be accessed using them**. Reducing the number of remote admin tools and their allowed access will increase visibility of unauthorized use of these tools.
- **Use encrypted services to protect network communications and disable all clear text administration services**(e.g., Telnet, HTTP, FTP, SNMP 1/2c). This ensures that sensitive information cannot be easily obtained by a threat actor capturing network traffic.

Implement a Mandatory Access Control Model

- **Implement stringent access controls to sensitive data and resources**. Access should be restricted to those users who require access and to the minimal level of access needed.

Audit Account Usage

- **Monitor VPN logins to look for suspicious access** (e.g., logins from unusual geo locations, remote logins from accounts not normally used for remote access, concurrent logins for the same account from different locations, unusual times of the day).
- **Closely monitor the use of administrative accounts**. Admin accounts should be used sparingly and only when necessary, such as installing new software or patches. Any use of admin accounts should be reviewed to determine if the activity is legitimate.
- **Ensure standard user accounts do not have elevated privileges** Any attempt to increase permissions on standard user accounts should be investigated as a potential compromise.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, CISA, FBI, and NSA recommend exercising, testing, and validating your organization's security program against threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. CISA, FBI, and NSA recommend 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 Table 1).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze the performance of your detection and prevention technologies.

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, FBI, and NSA recommend 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

CISA offers several no-cost scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors. See cisa.gov/cyber-hygiene-services.

U.S. DIB sector organizations may consider signing up for the NSA Cybersecurity Collaboration Center's DIB Cybersecurity Service Offerings, including Protective Domain Name System (PDNS) services, vulnerability scanning, and threat intelligence collaboration for eligible organizations. For more information on how to enroll in these services, email dib_defense@cyber.nsa.gov.

ACKNOWLEDGEMENTS

CISA, FBI, and NSA acknowledge Mandiant for its contributions to this CSA.