CYBERSECURITY ADVISORY

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

Last Revised: October 05, 2022 **Alert Code:** AA22-277A

Summary

Actions to Help Protect Against APT Cyber Activity:

- Enforce multifactor authentication (MFA) on all user accounts.
- Implement network segmentation to separate network segments based on role and functionality.
- Update software, including operating systems, applications, and firmware, on network assets.
- Audit account usage.

From November 2021 through January 2022, the Cybersecurity and Infrastructure Security Agency (CISA) responded to advanced persistent threat (APT) activity on a Defense Industrial Base (DIB) Sector organization's enterprise network. During incident response activities, CISA uncovered that likely multiple APT groups compromised the organization's network, and some APT actors had long-term access to the environment. APT actors used an open-source toolkit called Impacket to gain their foothold within the environment and further compromise the network, and also used a custom data exfiltration tool, CovalentStealer, to steal the victim's sensitive data.

This joint Cybersecurity Advisory (CSA) provides APT actors tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) identified during the incident response activities by CISA and a third-party incident response organization. The CSA includes detection and mitigation actions to help organizations detect and prevent related APT activity. CISA, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) recommend DIB sector and other critical infrastructure organizations implement the mitigations in this CSA to ensure they are managing and reducing the impact of cyber threats to their networks.

Download the PDF version of this report: pdf, 692 KB </sites/default/files/publications/aa22-277a-impacket-and-exfiltration-tool-used-to-steal-sensitive-information-from-defense-industrial-base-organization.pdf>

For a downloadable copy of IOCs, see the following files:

- Malware Analysis Report (MAR)-10365227-1.stix, 966 kb <https://www.cisa.gov/uscert/sites/default/files/publications/mar-10365227.r1.v1.white_stix_7.xml>
- MAR-10365227-2.stix, 249B <https://www.cisa.gov/uscert/sites/default/files/publications/mar-10365227.r2.v1.white_stix.xml>
- MAR-10365227-3.stix, 3.2 MB <https://www.cisa.gov/uscert/sites/default/files/publications/mar-10365227.r3.v1.white_stix_0.xml>

Technical Details

Threat Actor Activity

Note: *This advisory uses the MITRE ATT&CK® for Enterprise <https://attack.mitre.org/versions/v11/matrices/enterprise/> framework, version 11. See the MITRE ATT&CK Tactics and Techniques section for a table of the APT cyber activity mapped to MITRE ATT&CK for Enterprise framework.*

From November 2021 through January 2022, CISA conducted an incident response engagement on a DIB Sector organization's enterprise network. The victim organization also engaged a third-party incident response organization for assistance. During incident response activities, CISA and the trusted –third-party identified APT activity on the victim's network.

Some APT actors gained initial access to the organization's Microsoft Exchange Server as early as mid-January 2021. The initial access vector is unknown. Based on log analysis, the actors gathered information about the exchange environment and performed mailbox searches within a four-hour period after gaining access. In the same period, these actors used a compromised administrator account ("Admin 1") to access the EWS Application Programming Interface (API). In early February 2021, the actors returned to the network and used Admin 1 to access EWS API again. In both instances, the actors used a virtual private network (VPN).

Four days later, the APT actors used Windows Command Shell over a three-day period to interact with the victim's network. The actors used Command Shell to learn about the organization's environment and to collect sensitive data, including sensitive contract-related information from shared drives, for eventual exfiltration. The actors

manually collected files using the command-line tool, WinRAR. These files were split into approximately 3MB chunks located on the Microsoft Exchange server within the CU2\he\debug directory. See Appendix: Windows Command Shell Activity for additional information, including specific commands used.

During the same period, APT actors implanted Impacket <https://attack.mitre.org/versions/v11/software/s0357/>, a Python toolkit for programmatically constructing and manipulating network protocols, on another system. The actors used Impacket to attempt to move laterally to another system.

In early March 2021, APT actors exploited CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 to install 17 China Chopper webshells on the Exchange Server. Later in March, APT actors installed HyperBro on the Exchange Server and two other systems. For more information on the HyperBro and webshell samples, see CISA MAR-10365227-2 <https://www.cisa.gov/uscert/ncas/analysis-reports/ar22-277b> and -3 <https://www.cisa.gov/uscert/ncas/analysis-reports/ar22-277c>.

In April 2021, APT actors used Impacket for network exploitation activities. See the Use of Impacket section for additional information. From late July through mid-October 2021, APT actors employed a custom exfiltration tool, CovalentStealer, to exfiltrate the remaining sensitive files. See the Use of Custom Exfiltration Tool: CovalentStealer section for additional information.

APT actors maintained access through mid-January 2022, likely by relying on legitimate credentials.

Use of Impacket

CISA discovered activity indicating the use of two Impacket tools: wmiexec.py and smbexec.py. These tools use Windows Management Instrumentation (WMI) and Server Message Block (SMB) protocol, respectively, for creating a semi-interactive shell with the target device. Through the Command Shell, an Impacket user with credentials can run commands on the remote device using the Windows management protocols required to support an enterprise network.

The APT cyber actors used existing, compromised credentials with Impacket to access a higher privileged service account used by the organization's multifunctional devices. The threat actors first used the service account to remotely access the organization’s Microsoft Exchange server via Outlook Web Access (OWA) from multiple external IP addresses; shortly afterwards, the actors assigned the Application Impersonation role to the service account by running the following PowerShell command for managing Exchange:

powershell add-pssnapin *exchange*;New-ManagementRoleAssignment - name:"Journaling-Logs" -Role:ApplicationImpersonation -User:<account>

This command gave the service account the ability to access other users’ mailboxes.

The APT cyber actors used virtual private network (VPN) and virtual private server (VPS) providers, M247 and SurfShark, as part of their techniques to remotely access the Microsoft Exchange server. Use of these hosting providers, which serves to conceal interaction with victim networks, are common for these threat actors. According to CISA's analysis of the victim's Microsoft Exchange server Internet Information Services (IIS) logs, the actors used the account of a former employee to access the EWS. EWS enables access to mailbox items such as email messages, meetings, and contacts. The source IP address for these connections is mostly from the VPS hosting provider, M247.

Use of Custom Exfiltration Tool: CovalentStealer

The threat actors employed a custom exfiltration tool, CovalentStealer, to exfiltrate sensitive files.

CovalentStealer is designed to identify file shares on a system, categorize the files, and upload the files to a remote server. CovalentStealer includes two configurations that specifically target the victim's documents using predetermined files paths and user credentials. CovalentStealer stores the collected files on a Microsoft OneDrive cloud folder, includes a configuration file to specify the types of files to collect at specified times and uses a 256-bit AES key for encryption. See CISA MAR-10365227-1 <https://www.cisa.gov/uscert/ncas/analysis-reports/ar22-277a> for additional technical details, including IOCs and detection signatures.

MITRE ATT&CK Tactics and Techniques

MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. CISA uses the ATT&CK Framework as a foundation for the development of specific threat models and methodologies. Table 1 lists the ATT&CK techniques employed by the APT actors.

Table 1: Identified APT Enterprise ATT&CK Tactics and Techniques

Initial Access		
Technique Title	**ID**	**Use**

Valid Accounts	T1078 <https://attack.mitre.org/versions/v11/techniques/t1078/>	Actors obtained and abused credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. In this case, they exploited an organization's multifunctional device domain account used to access the organization's Microsoft Exchange server via OWA.

Execution

Technique Title	ID	Use
Windows Management Instrumentation	T1047 <https://attack.mitre.org/versions/v11/techniques/t1047/>	Actors used Impacket tools wmiexec.py and smbexec.py to leverage Windows Management Instrumentation and execute malicious commands.

Command and Scripting Interpreter	T1059 <https://attack.mitre.org/versions/v11/techniques/t1059/003/>	Actors abused command and script interpreters to execute commands.
Command and Scripting Interpreter: PowerShell	T1059.001 <https://attack.mitre.org/techniques/t1059/001>	Actors abused **PowerShell** commands and scripts to map shared drives by specifying a path to one location and retrieving the items from another. See Appendix: Windows Command Shell Activity for additional information.

Command and Scripting Interpreter: Windows Command Shell	T1059.003 <https://attack.mitre.org/versions/v11/techniques/t1059/003/>	Actors abused the **Windows Command Shell** to learn about the organization's environment and to collect sensitive data. See Appendix: Windows Command Shell Activity for additional information, including specific commands used. The actors used Impacket tools, which enable a user with credentials to run commands on the remote device through the Command Shell.
Command and Scripting Interpreter: Python	T1059.006 <https://attack.mitre.org/versions/v11/techniques/t1059/006/>	The actors used two Impacket tools: wmiexec.py and smbexec.py.

Shared Modules	T1129 <https://attack.mitre.org/techniques/t1129>	Actors executed malicious payloads via loading shared modules. The Windows module loader can be instructed to load DLLs from arbitrary local paths and arbitrary Universal Naming Convention (UNC) network paths.
System Services	T1569 <https://attack.mitre.org/versions/v11/techniques/t1569/>	Actors abused system services to execute commands or programs on the victim's network.

Persistence

Technique Title	ID	Use
Valid Accounts	T1078 <https://attack.mitre.org/versions/v11/techniques/t1078/>	Actors obtained and abused credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.

Create or Modify System Process	T1543 <https://attack.mitre.org/versions/v11/techniques/t1543/>	Actors were observed creating or modifying system processes.

Privilege Escalation

Technique Title	ID	Use
Valid Accounts	T1078 <https://attack.mitre.org/versions/v11/techniques/t1078/>	Actors obtained and abused credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. In this case, they exploited an organization's multifunctional device domain account used to access the organization's Microsoft Exchange server via OWA.

Defense Evasion

Technique Title	ID	Use

Masquerading: Match Legitimate Name or Location	T1036.005 <https://attack.mitre.org/versions/v11/techniques/t1036/005>	Actors masqueraded the archive utility WinRAR.exe by renaming it VMware.exe to evade defenses and observation.
Indicator Removal on Host	T1070 <https://attack.mitre.org/versions/v11/techniques/t1070/004/>	Actors deleted or modified artifacts generated on a host system to remove evidence of their presence or hinder defenses.
Indicator Removal on Host: File Deletion	T1070.004 <https://attack.mitre.org/versions/v11/techniques/t1070/004/>	Actors used the del.exe command with the /f parameter to force the deletion of read-only files with the *.rar and tempg* wildcards.

Valid Accounts	T1078 <https://attack.mitre.org/versions/v11/techniques/t1078/>	Actors obtained and abused credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. In this case, they exploited an organization's multifunctional device domain account used to access the organization's Microsoft Exchange server via OWA.
Virtualization/Sandbox Evasion: System Checks	T1497.001 <https://attack.mitre.org/techniques/t1497/001>	Actors used **Windows command shell** commands to detect and avoid virtualization and analysis environments. See Appendix: Windows Command Shell Activity for additional information.

Impair Defenses: Disable or Modify Tools	T1562.001 <https://attack.mitre.org/techniques/t1562/001>	Actors used the taskkill command to probably disable security features. CISA was unable to determine which application was associated with the Process ID.
Hijack Execution Flow	T1574 <https://attack.mitre.org/versions/v11/techniques/t1574/>	Actors were observed using hijack execution flow.

Discovery

Technique Title	ID	Use
System Network Configuration Discovery	T1016 <https://attack.mitre.org/techniques/t1016>	Actors used the systeminfo command to look for details about the network configurations and settings and determine if the system was a VMware virtual machine. The threat actor used route print to display the entries in the local IP routing table.

System Network Configuration Discovery: Internet Connection Discovery	T1016.001 <https://attack.mitre.org/techniques/t1016/001>	Actors checked for internet connectivity on compromised systems. This may be performed during automated discovery and can be accomplished in numerous ways.
System Owner/User Discovery	T1033 <https://attack.mitre.org/techniques/t1033>	Actors attempted to identify the primary user, currently logged in user, set of users that commonly use a system, or whether a user is actively using the system.
System Network Connections Discovery	T1049 <https://attack.mitre.org/techniques/t1049>	Actors used the netstat command to display TCP connections, prevent hostname determination of foreign IP addresses, and specify the protocol for TCP.

Process Discovery	T1057 <https://attack.mitre.org/techniques/t1057>	Actors used the tasklist command to get information about running processes on a system and determine if the system was a VMware virtual machine. The actors used tasklist.exe and find.exe to display a list of applications and services with their PIDs for all tasks running on the computer matching the string “powers.”
System Information Discovery	T1082 <https://attack.mitre.org/techniques/t1082>	Actors used the ipconfig command to get detailed information about the operating system and hardware and determine if the system was a VMware virtual machine.

File and Directory Discovery	T1083 <https://attack.mitre.org/techniques/t1083>	Actors enumerated files and directories or may search in specific locations of a host or network share for certain information within a file system.
Virtualization/Sandbox Evasion: System Checks	T1497.001 <https://attack.mitre.org/techniques/t1497/001>	Actors used Windows command shell commands to detect and avoid virtualization and analysis environments.

Lateral Movement

Technique Title	ID	Use
Remote Services: SMB/Windows Admin Shares	T1021.002 <https://attack.mitre.org/techniques/t1021/002>	Actors used Valid Accounts to interact with a remote network share using Server Message Block (SMB) and then perform actions as the logged-on user.

Collection

Technique Title	ID	Use

Archive Collected Data: Archive via Utility	T1560.001 <https://attack.mitre.org/techniques/t1560>	Actor used PowerShell commands and WinRAR to compress and/or encrypt collected data prior to exfiltration.

Data from Network Shared Drive	T1039 <https://attack.mitre.org/versions/v11/techniques/t1039/>	Actors likely used net share command to display information about shared resources on the local computer and decide which directories to exploit, the powershell dir command to map shared drives to a specified path and retrieve items from another, and the ntfsinfo command to search network shares on computers they have compromised to find files of interest. The actors used dir.exe to display a list of a directory's files and subdirectories matching a certain text string.

Data Staged: Remote Data Staging	T1074.002 <https://attack.mitre.org/versions/v11/techniques/t1074/002/>	The actors split collected files into approximately 3 MB chunks located on the Exchange server within the CU2\he\debug directory.
Command and Control		
Technique Title	**ID**	**Use**
Non-Application Layer Protocol	T1095 <https://attack.mitre.org/techniques/t1095>	Actors used a non-application layer protocol for communication between host and Command and Control (C2) server or among infected hosts within a network.
Ingress Tool Transfer	T1105 <https://attack.mitre.org/versions/v11/techniques/t1105/>	Actors used the certutil command with three switches to test if they could download files from the internet. The actors employed CovalentStealer to exfiltrate the files.

Proxy	T1090 <https://attack.mitre.org/versions/v11/techniques/t1090/>	Actors are known to use VPN and VPS providers, namely M247 and SurfShark, as part of their techniques to access a network remotely.

Exfiltration

Technique Title	ID	Use
Schedule Transfer	T1029 <https://attack.mitre.org/versions/v11/techniques/t1029/>	Actors scheduled data exfiltration to be performed only at certain times of day or at certain intervals and blend traffic patterns with normal activity.
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002 <https://attack.mitre.org/versions/v11/techniques/t1567/002>	The actor's CovalentStealer tool stores collected files on a Microsoft OneDrive cloud folder.

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 (SayCISA@cisa.dhs.gov or 1-844-Say-CISA).
  - Report incidents to your local FBI field office at fbi.gov/contact-us/field-offices <http://www.fbi.gov/contact-us/field> 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 <https://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 <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/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 <https://media.defense.gov/2022/jun/22/2003021689/-1/-1/1/csi_keeping_powershell_security_measures_to_use_and_embrace_20220622.pdf>.

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 <https://media.defense.gov/2019/sep/09/2002180325/-1/-1/0/segment%20networks%20and%20deploy%20application%20aware%20defenses%20-%20copy.pdf>.)
- **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 <https://www.cisa.gov/known-exploited-vulnerabilities-catalog> 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 <https://www.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.

APPENDIX: WINDOWS COMMAND SHELL ACTIVITY

Over a three-day period in February 2021, APT cyber actors used Windows Command Shell to interact with the victim's environment. When interacting with the victim's system and executing commands, the threat actors used /q and /c parameters to turn the echo off, carry out the command specified by a string, and stop its execution once

completed.

On the first day, the threat actors consecutively executed many commands within the Windows Command Shell to learn about the organization's environment and to collect sensitive data for eventual exfiltration (see Table 2).

Table 2: Windows Command Shell Activity (Day 1)

Command	Description / Use
net share	Used to create, configure, and delete network shares from the command-line.[1 <https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh750728(v=ws.11)>] The threat actor likely used this command to display information about shared resources on the local computer and decide which directories to exploit.
powershell dir	An alias (shorthand) for the PowerShell Get-ChildItem cmdlet. This command maps shared drives by specifying a path to one location and retrieving the items from another.[2] The threat actor added additional switches (aka options, parameters, or flags) to form a "one liner," an expression to describe commonly used commands used in exploitation: powershell dir -recurse -path e:\<redacted>|select fullname,length|export-csv c:\windows\temp\temp.txt. This particular command lists subdirectories of the target environment when.
systeminfo	Displays detailed configuration information [3 <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/systeminfo>], tasklist – lists currently running processes [4 <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/tasklist>], and ipconfig – displays all current Transmission Control Protocol (TCP)/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings, respectively [5 <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig>]. The threat actor used these commands with specific switches to determine if the system was a VMware virtual machine: systeminfo > vmware & date /T, tasklist /v > vmware & date /T, and ipconfig /all >> vmware & date /.
route print	Used to display and modify the entries in the local IP routing table. [6 <https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/ff961510(v=ws.11)>] The threat actor used this command to display the entries in the local IP routing table.
netstat	Used to display active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics, and IPv6 statistics.[7 <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat>] The threat actor used this command with three switches to display TCP connections, prevent hostname determination of foreign IP addresses, and specify the protocol for TCP: netstat -anp tcp.

certutil	Used to dump and display certification authority (CA) configuration information, configure Certificate Services, backup and restore CA components, and verify certificates, key pairs, and certificate chains.[8 <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certutil>] The threat actor used this command with three switches to test if they could download files from the internet: certutil -urlcache -split -f https://microsoft.com temp.html.
ping	Sends Internet Control Message Protocol (ICMP) echoes to verify connectivity to another TCP/IP computer.[9 <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ping>] The threat actor used ping -n 2 apple.com to either test their internet connection or to detect and avoid virtualization and analysis environments or network restrictions.
taskkill	Used to end tasks or processes.[10 <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/taskkill>] The threat actor used taskkill /F /PID 8952 to probably disable security features. CISA was unable to determine what this process was as the process identifier (PID) numbers are dynamic.
PowerShell Compress-Archive cmdlet	Used to create a compressed archive or to zip files from specified files and directories.[11] The threat actor used parameters indicating shared drives as file and folder sources and the destination archive as zipped files. Specifically, they collected sensitive contract-related information from the shared drives.

On the second day, the APT cyber actors executed the commands in Table 3 to perform discovery as well as collect and archive data.

Table 3: Windows Command Shell Activity (Day 2)

Command	Description / Use
ntfsinfo.exe	Used to obtain volume information from the New Technology File System (NTFS) and to print it along with a directory dump of NTFS meta-data files.[12 <https://docs.microsoft.com/en-us/sysinternals/downloads/ntfsinfo>]
WinRAR.exe	Used to compress files and subsequently masqueraded WinRAR.exe by renaming it VMware.exe.[13 <https://www.rarlab.com/>]

On the third day, the APT cyber actors returned to the organization's network and executed the commands in Table 4.

Table 4: Windows Command Shell Activity (Day 3)

Command	Description / Use
powershell -ep bypass import-module .\vmware.ps1;export-mft -volume e	Threat actors ran a PowerShell command with parameters to change the execution mode and bypass the Execution Policy to run the script from PowerShell and add a module to the current section: powershell -ep bypass import-module .\vmware.ps1;export-mft -volume e. This module appears to acquire and export the Master File Table (MFT) for volume E for further analysis by the cyber actor.[14]
set.exe	Used to display the current environment variable settings.[15 <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/set_1>] (An environment variable is a dynamic value pointing to system or user environments (folders) of the system. System environment variables are defined by the system and used globally by all users, while user environment variables are only used by the user who declared that variable and they override the system environment variables (even if the variables are named the same).
dir.exe	Used to display a list of a directory's files and subdirectories matching the eagx* text string, likely to confirm the existence of such file.
tasklist.exe and find.exe	Used to display a list of applications and services with their PIDs for all tasks running on the computer matching the string “powers”.[16 <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/tasklist>][17 <https://attack.mitre.org/software/s0057/>][18 <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/find>]
ping.exe	Used to send two ICMP echos to amazon.com. This could have been to detect or avoid virtualization and analysis environments, circumvent network restrictions, or test their internet connection.[19 <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ping>]
del.exe with the /f parameter	Used to force the deletion of read-only files with the *.rar and tempg* wildcards.[20 <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/del>]

References

[1] Microsoft Net Share <https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh750728(v=ws.11)>

[2] Microsoft Get-ChildItem

[3] Microsoft systeminfo <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/systeminfo>

[4] Microsoft tasklist <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/tasklist>
[5] Microsoft ipconfig <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig>
[6] Microsoft Route <https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/ff961510(v=ws.11)>
[7] Microsoft netstat <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat>
[8] Microsoft certutil <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certutil>
[9] Microsoft ping <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ping>
[10] Microsoft taskkill <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/taskkill>
[11] Microsoft Compress-Archive
[12] NTFSInfo v1.2 <https://docs.microsoft.com/en-us/sysinternals/downloads/ntfsinfo>
[13] rarlab <https://www.rarlab.com/>
[14] Microsoft Import-Module
[15] Microsoft set (environment variable) <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/set_1>
[16] Microsoft tasklist <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/tasklist>
[17] Mitre ATT&CK - Sofware: TaskList <https://attack.mitre.org/versions/v11/software/s0057/>
[18] Microsoft find <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/find>
[19] Microsoft ping <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ping>
[20] Microsoft del <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/del>

Revisions

October 4, 2022: Initial version