China APT's, Volt Typhoon, and what to do!

Shannon Davis, Principal Security Strategist,
Splunk SURGe

Mike Trewartha, Senior Incident Response Consultant,
Cisco Talos

August 2024

Threat Actor Overview

Threat Actor Naming Guide

Adversary	Nation-state or Category
BEAR	RUSSIA
BUFFALO	VIETNAM
CHOLLIMA	DPRK (NORTH KOREA)
CRANE	ROK (REPUBLIC OF KOREA)
JACKAL	HACKTIVIST
KITTEN	IRAN
LEOPARD	PAKISTAN
LYNX	GEORGIA
OCELOT	COLOMBIA
PANDA	PEOPLE'S REPUBLIC OF CHINA
SPIDER	ECRIME
TIGER	INDIA
WOLF	TURKEY

China Affiliated Threat Actors

APT1	APT2	APT3	APT4	APT5	APT6	APT7	APT8	APT10	APT12	APT14
• Unit 61398 • Comment Panda • Comment Crew • Byzantine Candor • TG-8223	• Putter Panda • Unit 61486 • Sulphur • TG-6952 • G0024	• UPS Team • Boyusec • Gothic Panda • Buckeye	• Maverick Panda • Sykipot Group Wisp • TG-0623 • Bronze Editions	• Manganes • UNC2630 • Keyhole Panda				• Menupass • Cicada • Cloud Hopper • Red Apollo • Stone Panda • POTASSIUM • BRONZE RIVERSIDE	• Calc Team • Numbered Panda • IXESHE • JOYRAT • DynCalc • BRONZE GLOBE	• Anchor Panda

APT15	APT16	APT17	APT19	APT20	APT21	APT22	APT23	APT24	APT26	APT27
• PlayfulTaurus • Vixen Panda • Ke3Chan • Nickel • BackdoorDiplomac • Red Vulture • Nylon Typhoon	• SVCMONDR • G0023	• Tailgator Team • Deputy Dog	• Codoso Team	• Twivy • Violin Panda • Crawling Taurus	• Zhenbao • HAMMER PANDA • TEMP.Zhenbao • NetTraveler	• Barista	• Tropic Trooper • Pirate Panda • KeyBoy • BRONZE HOBART • Red Orthrus • Earth Centaur	• PittyTiger	• BronzeEmpress • Turbine Panda	• Emissary Panda • Lucky Mouse • TEMP.Hippo • GreedyTaotie • TG-3390 • Red Phoenix • Iron Tiger • BRONZE UNION • G0027 • Iron Taurus

APT30	APT31	APT40	APT41	Black Tech	Bronze Starlight	Conference Crew	Cycldek	Dark Shadow	Deep Panda	Dragon OK
• Naikon • PLA Unit 78020 • Lotus Panda • Firefly	• Zirconium • Judgement Panda	• GADOLINIUM • MudCarp • BRONZE MOHAWK • Kryptonite Panda • Leviathan • Temp.Periscope	• Tailgator Team • Deputy Dog	• Circuit Panda • Mobwork • Palmerworm • Red Dijinn • HUAPI • Manga Taurus • Earth Hundun	• DEV-0401		• Goblin Panda • Conimes	• Storm-0062 • Oro0lxy	• Shell Crew • WebMasters • KungFu Kittens • PinkPanther • Black Vine	• TBA

Earth Krahang	Earth Lusca	Flax Typhoon	Gallium	Ghost Emperor	Hafnium	Honker Union	Lilac Typhoon	LouYu	Muddling Meerkat	Mustang Panda
	• TAG-22 • G1006	• Ethereal Panda • RedJuliett • TAG-91	• Red Dev 4 • Alloy Taurus • Granite Typhoon				• DEV-0234			• Bronze President • RedDelta • TA426 • HoneyMyte • Temp.Hex • Fireant

Nomad Panda	Roaming Tiger	Sharp Dragon	Toddy Cat	Tonto Team	UNC4191	Velvet Ant	Volt Typhoon
• RedFoxtrot • Neeedleminer		• Sharp Panda		• Karma Panda • CactusPete • Bronze Huntley • Red Beifang • G0131			• Voltzite • Vanguard Panda • Bronze Silhouette • Dev-0391 • UNC3236 • Insidious Taurus

Volt Typhoon

Volt Typhoon

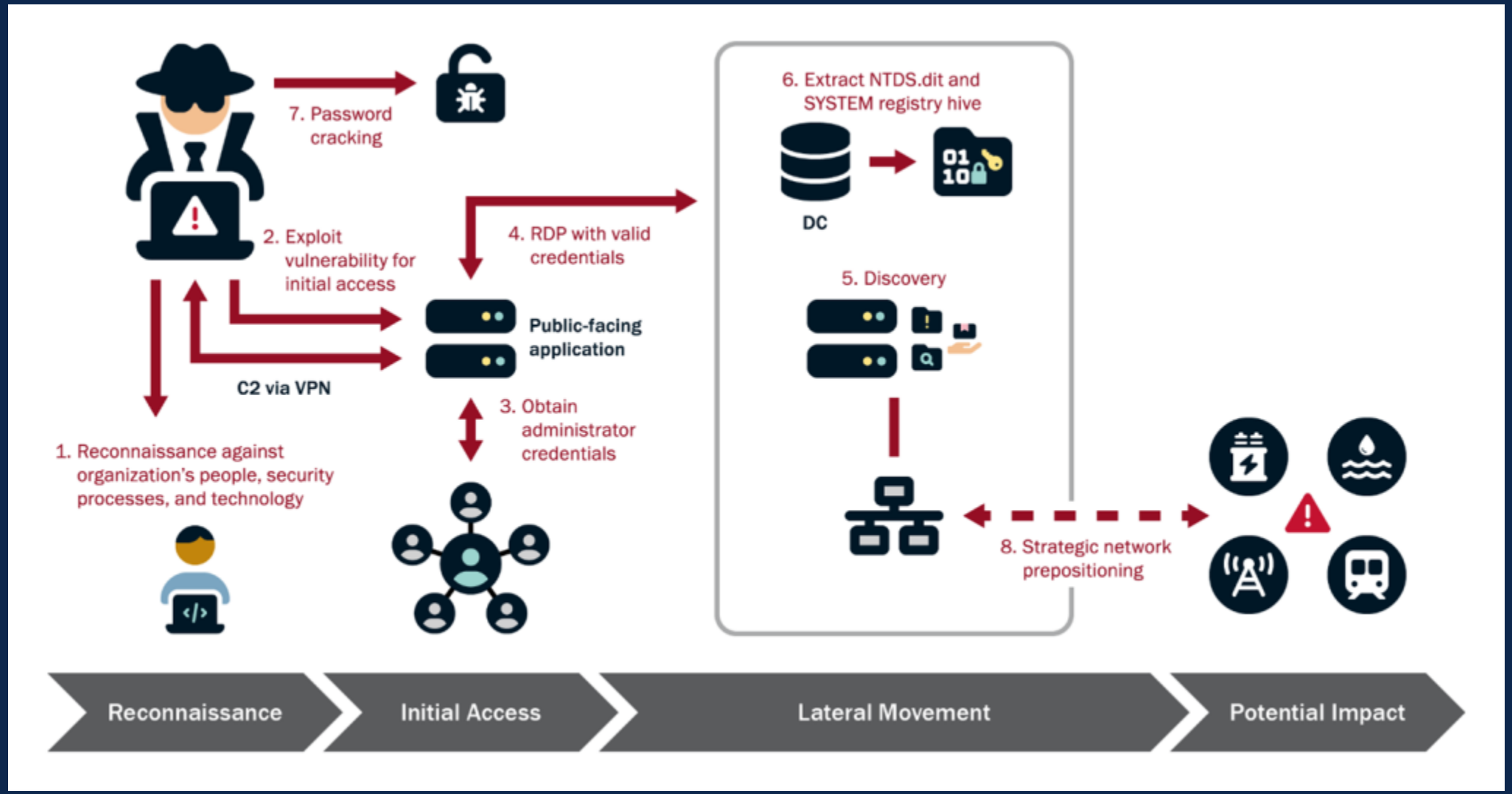
Energy

Water and
Wastewater Systems

Transportation

Communications

Volt Typhoon: Overview of Activity



Source: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

Volt Typhoon: TTPs

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0003: Persistence
T1591: Gather Victim Org Information	T1090.003: Proxy: Multi-hop Proxy	T1190: Exploit Public-Facing Application	T1133: External Remote Services
T1590: Gather Victim Network Information	T1583.003: Acquire Infrastructure: Botnet	T1588.005: Obtain Capabilities: Exploits	T1078: Valid Accounts
T1589: Gather Victim Identity Information	T1584.005: Compromise Infrastructure: Botnet	T1587.004: Develop Capabilities: Exploits	
T1593: Search Open Websites/Domains			
T1594: Search Victim-Owned Websites			
T1592: Gather Victim Host Information			
T1589.002 Gather Victim Identity Information: Email Addresses			

Volt Typhoon: TTPs

TA0002: Execution	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery
T1059: Command and Scripting Interpreter	T1027.002: Obfuscated Files or Information: Software Packaging	T1068: Exploitation for Privilege Escalation	T1082: System Information Discovery
T1218: System Binary Proxy Execution	T1070.001: Indicator Removal: Clear Windows Event Logs	T1552: Unsecured Credentials	T1046: Network Service Discovery
T1105: Ingress Tool Transfer	T1070.009: Indicator Removal: Clear Persistence	T1003.003: OS Credential Dumping: NTDS	T1069: Permission Groups Discovery
T1003.001: OS Credential Dumping: LSASS Memory	T1036.005: Masquerading: Match Legitimate Name or Location	T1021.001: Remote Services: Remote Desktop Protocol	T1033: System Owner/User Discovery
	T1070.004: Indicator Removal: File Deletion	T1006: Direct Volume Access	T1654: Log Enumeration
		T1047: Windows Management Instrumentation	T1057: Process Discovery
		T1110.002: Brute Force: Password Cracking	T1010: Application Window Discovery
		T1012: Query Registry	T1016.001: System Network Configuration Discovery: Internet Connection Discovery
			T1007: System Service Discovery
			T1083: File and Directory Discovery

Volt Typhoon: TTPs

TA008: Lateral Movement	TA0009: Collection & TA0010: Exfiltration	TA0011: Command and Control (C2)
T1550: Use Alternate Authentication Method	T1560: Archive Collected Data	T1090: Proxy
T1563: Remote Service Session Hijacking	T1048: Exfiltration Over Alternative Protocol	T1573: Encrypted Channel
T1021.007 Remote Services: Cloud Services	T1560.001: Archive Collected Data: Archive via Utility	T1059.001: Command and Scripting Internpreter: PowerShell
T1078:004 Valid Accounts: Cloud Accounts		T1016: System Network Configuration Discovery
		T1059.004: Command and Scripting Interpreter: Unix Shell
		T1112: Modify Registry
		T:1090.001: Proxy: Internal Proxy
		T:1584.004: Compromised Infrastructure: Server

Volt Typhoon: Recommendations

Detection & Hunting Recommendations:

- Apply Living off the Land Detection Best Practices
- Routinely review application, security, and system event logs, focusing on Windows Extensible Storage Engine Technology (ESENT) Application Logs
- Monitor and Review OT System Logs
- Monitor for Possible Network Proxy Activity
- Review Logins for Impossible Travel
- Review Standard Directories for Unusual Files
  - **`C:\windows\temp\`**
  - **`C:\users\public\`**

Mitigations:

- Harden the Attack Surface
- Secure Credentials
- Secure Accounts
- Secure Remote Access Services
- Secure Sensitive Data
- Implement Network Segmentation
- Secure Cloud Assets
- Revoke unnecessary public access to cloud environment

- Be Prepared!!!

Whoami

Shannon Davis
Principal Security Strategist
Splunk SURGe

- Based in Melbourne since 2001
- Originally from Seattle
- Responsible for SURGe in APAC

Expertise to help solve security problems

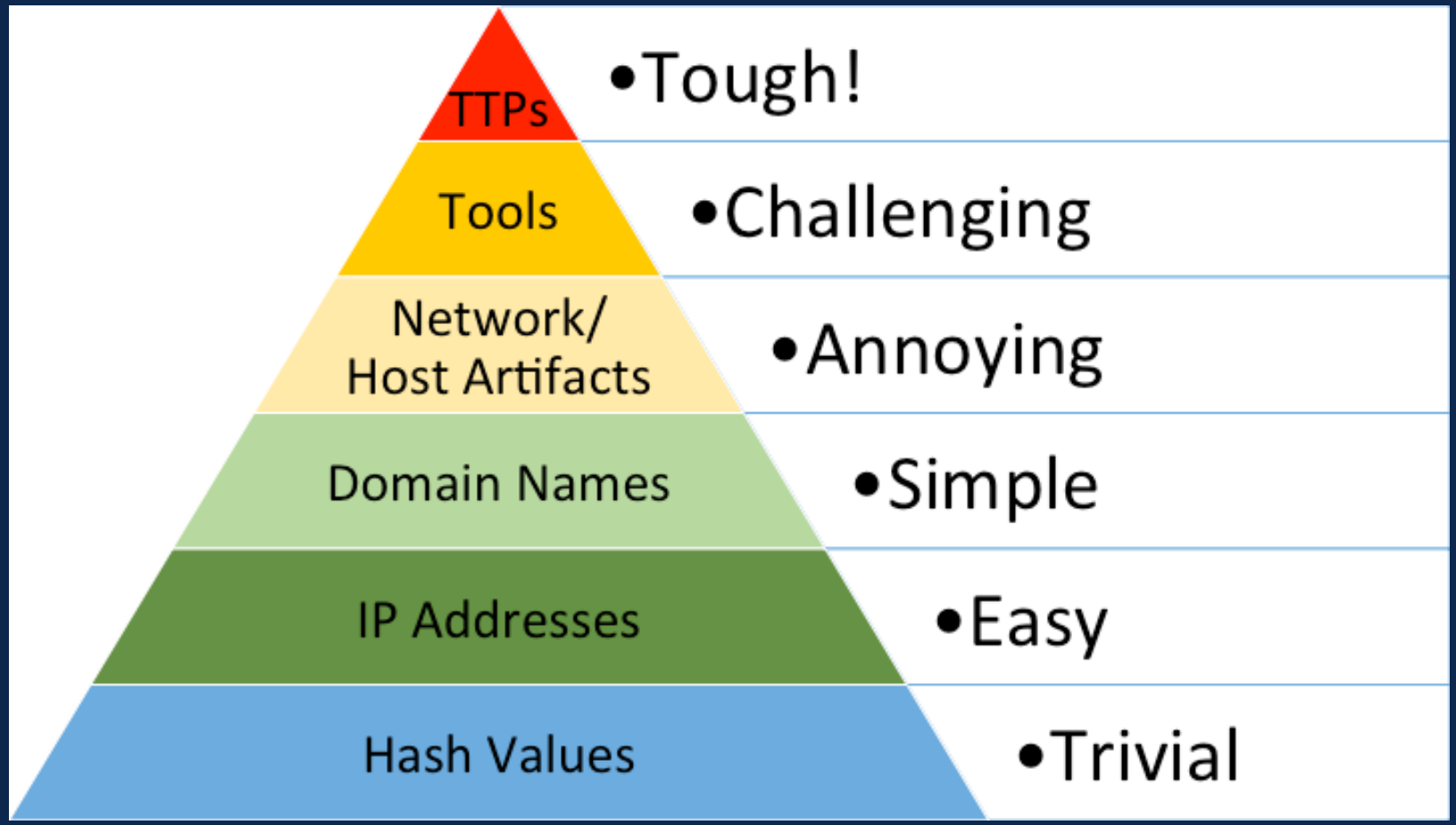
The SURGe team focuses on in-depth analysis of the latest cybersecurity news and finding answers to security problems. All of this is delivered to you in the form of research, rapid response guides, suggested reading and events.

https://www.splunk.com/en_us/surge.html

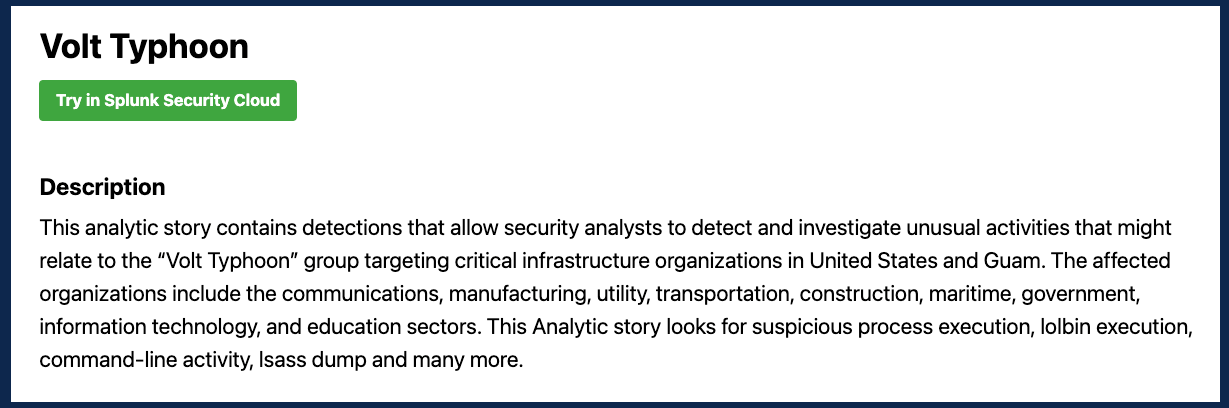
Eat Your Cyber Veggies

- Patching
- MFA
- Endpoint Protection (EDR/XDR)
- Allowlisting
- Centralised Logging
  - Endpoint
    - Sysmon
    - PowerShell
  - Authentication
    - AD
    - Duo/Okta/etc

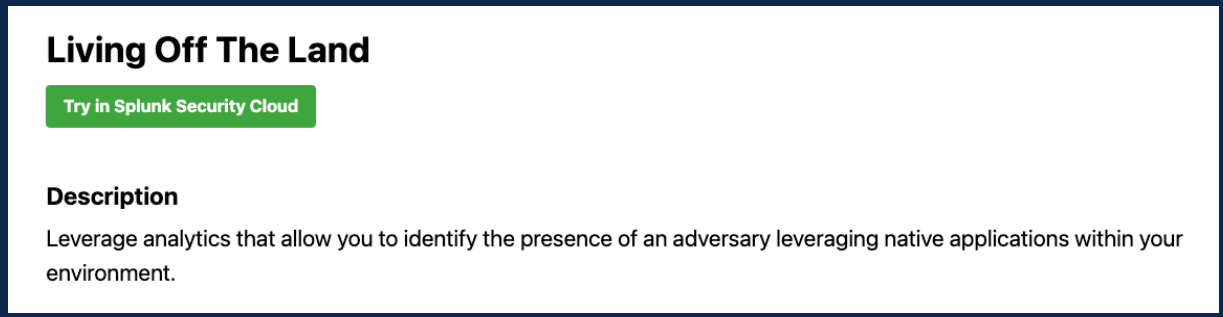
Behave Yourself



Analytic Stories



https://research.splunk.com/stories/volt_typhoon/



https://research.splunk.com/stories/living_off_the_land/

Detections

Name	Technique	Type
Cmdline Tool Not Executed In CMD Shell	Command and Scripting Interpreter, JavaScript	TTP
Creation of Shadow Copy	NTDS, OS Credential Dumping	TTP
Creation of Shadow Copy with wmic and powershell	NTDS, OS Credential Dumping	TTP
Detect PsExec With accepteula Flag	Remote Services, SMB/Windows Admin Shares	TTP
Dump LSASS via comsvcs DLL	LSASS Memory, OS Credential Dumping	TTP
Elevated Group Discovery With Net	Permission Groups Discovery, Domain Groups	TTP
Executables Or Script Creation In Suspicious Path	Masquerading	Anomaly
Extraction of Registry Hives	Security Account Manager, OS Credential Dumping	TTP
Impacket Lateral Movement Commandline Parameters	Remote Services, SMB/Windows Admin Shares, Distributed Component Object Model, Windows Management Instrumentation, Windows Service	TTP
Impacket Lateral Movement WMIExec Commandline Parameters	Remote Services, SMB/Windows Admin Shares, Distributed Component Object Model, Windows Management Instrumentation, Windows Service	TTP
Impacket Lateral Movement WMIExec Commandline Parameters	Remote Services, SMB/Windows Admin Shares, Distributed Component Object Model, Windows Management Instrumentation, Windows Service	TTP
Impacket Lateral Movement smbexec CommandLine Parameters	Remote Services, SMB/Windows Admin Shares, Distributed Component Object Model, Windows Management Instrumentation, Windows Service	TTP
Impacket Lateral Movement smbexec CommandLine Parameters	Remote Services, SMB/Windows Admin Shares, Distributed Component Object Model, Windows Management Instrumentation, Windows Service	TTP
Malicious PowerShell Process - Encoded Command	Obfuscated Files or Information	Hunting
Malicious PowerShell Process - Execution Policy Bypass	Command and Scripting Interpreter, PowerShell	TTP
Net Localgroup Discovery	Permission Groups Discovery, Local Groups	Hunting

Example
(Command Line Tool Not Executed in Command Line)

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes where
(Processes.process_name = "ipconfig.exe" OR Processes.process_name = "systeminfo.exe" OR Processes.process_name = "net.exe" OR
Processes.process_name = "net1.exe" OR Processes.process_name = "arp.exe" OR Processes.process_name = "nslookup.exe" OR Processes.process_name =
"route.exe" OR Processes.process_name = "netstat.exe" OR Processes.process_name = "whoami.exe") AND NOT (Processes.parent_process_name = "cmd.exe"
OR Processes.parent_process_name = "powershell*" OR Processes.parent_process_name="pwsh.exe" OR Processes.parent_process_name = "explorer.exe") by
Processes.parent_process_name Processes.parent_process Processes.process_name Processes.original_file_name Processes.process_id Processes.process
Processes.dest Processes.user
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `cmdline_tool_not_executed_in_cmd_shell_filter`
```

Parent Process
!=
cmd.exe
powershell
explorer

nslookup.exe
route.exe
netstat.exe
whoami.exe

Example
(Elevated Group Discovery with Net Commands)

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes where
(Processes.process_name="net.exe" OR Processes.process_name="net1.exe") (Processes.process="*group*" AND Processes.process="*/do*")
(Processes.process="*Domain Admins*" OR Processes.process="*Enterprise Admins*" OR Processes.process="*Schema Admins*" OR
Processes.process="*Account Operators*" OR Processes.process="*Server Operators*" OR Processes.process="*Protected Users*" OR Processes.process="*Dns
Admins*") by Processes.dest Processes.user Processes.parent_process Processes.process_name Processes.process Processes.process_id
Processes.parent_process_id
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `elevated_group_discovery_with_net_filter`
```

Net or Net1
+ group

"Domain Admins" /domain
"Enterprise Admins" /domain
"Schema Admins" /domain
"Account Operators" /domain
"Server Operators" /domain
"Protected Users" /domain
"Dns Admins" /domain

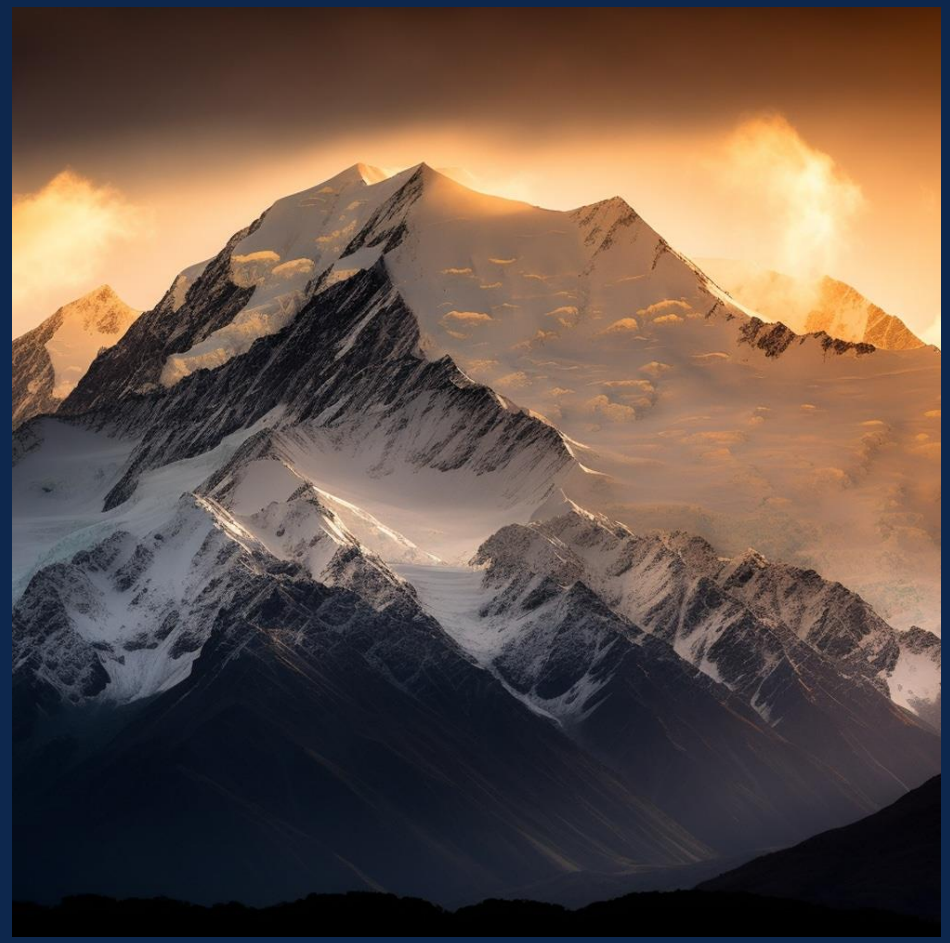
Macro-level ATT&CK Trends

Top Consensus Technique Reporting in 2023

Technique	Avg. Freq.	Reported by
T1059.001 Command and Scripting Interpreter: PowerShell	29.9 %	CISA, M-Trends, Red Canary
T1027 Obfuscated Files or Information	29.1 %	CISA, M-Trends, Red Canary
T1105 Ingress Tool Transfer	28.0 %	CISA, M-Trends, Red Canary
T1055 Process Injection	15.6 %	CISA, M-Trends, Red Canary

https://www.splunk.com/en_us/blog/security/revisiting-the-big-picture-macro-level-att-ck-updates-for-2023.html

PEAK Threat Hunting Framework



PEAK eBook
(Not Malicious, I Promise)

The bridge to possible