Mandiant

VHR20260603 - JUNE 3, 2026

The Mandiant Intelligence Validation Research Team (VRT) has published VHR20260603 - Content Expansion. This content pack requires Director version 4.14.1.0-0 or higher.

If you've enabled the Content Service, this content pack will automatically download and be applied to your Director (see **The Mandiant Content Service** (https://docs.mandiant.com/home/msv-mandiant-content-service) and **Managing Security Validation Content** (https://docs.mandiant.com/home/msv-content-settings) for full details). Otherwise, you can download the **security content pack** (https://docs.mandiant.com/home/msv-content-packs) from the Mandiant Documentation Portal.

Summary of Changes

- 83 Actions added
- 61 Files added
- 7 Actions updated
- 1 Files updated

Release Highlights

- New Actions covering **Campaign 26-053** (https://advantage.mandiant.com/campaigns/CAMP.26.053), a campaign targeting healthcare and education with obfuscated PowerShell, registry modifications, and discovery via tools such as **NLTEST** (https://advantage.mandiant.com/malware/NLTEST).
- New Actions covering **Campaign 26-054** (https://advantage.mandiant.com/campaigns/CAMP.26.054), a China-nexus threat actor **UNC6863** (https://advantage.mandiant.com/actors/UNC6863) campaign deploying **SLICKDEMON** (https://advantage.mandiant.com/malware/SLICKDEMON) and **BADFALL** (https://advantage.mandiant.com/malware/BADFALL) (QUIC RAT) via software supply chain compromise of DAEMON Tools.
- A new Action demonstrating **Campaign 26-052** (https://advantage.mandiant.com/campaigns/CAMP.26.052), a financially motivated actor **UNC6780** (https://advantage.mandiant.com/actors/UNC6780) campaign poisoning software supply chains to compromise CI/CD environments via **DUSTMAKER** (https://advantage.mandiant.com/malware/DUSTMAKER) and **SANDCLOCK** (https://advantage.mandiant.com/malware/SANDCLOCK).
- A new Action demonstrating **Campaign 26-055** (https://advantage.mandiant.com/campaigns/CAMP.26.055), a campaign by an Actor of Unknown Motivations leveraging ClickFix phishing lures to target multiple organizations, via **BLACKWIDOW** (https://advantage.mandiant.com/malware/BLACKWIDOW).
- A new Action covering **Campaign 26-058** (https://advantage.mandiant.com/campaigns/CAMP.26.058), describing the deployment of the **XMRIG** (https://advantage.mandiant.com/malware/XMRIG) cryptocurrency miner via masqueraded PowerShell.
- New Actions demonstrating **Campaign 26-057** (https://advantage.mandiant.com/campaigns/CAMP.26.057), a campaign involving **UNC6847** (https://advantage.mandiant.com/actors/UNC6847) using **FLINTWIRE** (https://advantage.mandiant.com/malware/FLINTWIRE) and **ADAPTAGENT** (https://advantage.mandiant.com/malware/ADAPTAGENT) for PowerShell-based fileless execution and multiple persistence mechanisms.
- New Actions demonstrating **Campaign 26-059** (https://advantage.mandiant.com/campaigns/CAMP.26.059), a campaign deploying **VIDAR** (https://advantage.mandiant.com/malware/VIDAR) infostealer via **NEONSLIDE** (https://advantage.mandiant.com/malware/NEONSLIDE) PowerShell Downloader.
- New Actions demonstrating **Campaign 26-060** (https://advantage.mandiant.com/campaigns/CAMP.26.060), a financially motivated software supply chain attack by **UNC6780** (https://advantage.mandiant.com/actors/UNC6780) leveraging GitHub Actions cache poisoning and malicious PyPI packages to deploy the **FIRESCALE** (https://advantage.mandiant.com/malware/FIRESCALE) credential stealer.
- New Actions demonstrating **Campaign 26-062** (https://advantage.mandiant.com/campaigns/CAMP.26.062), an East Europe-Nexus financial gain actor's campaign deploying **ETHERRAT** (https://advantage.mandiant.com/malware/ETHERRAT) and **MATANBUCHUS** (https://advantage.mandiant.com/malware/MATANBUCHUS) via Trojanized Installer.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

- A new Action covering **CVE-2026-0300** (https://advantage.mandiant.com/vulnerabilities/CVE-2026-0300), an Out-of-bounds Write vulnerability in Palo Alto Networks PAN-OS that allows unauthenticated remote code execution and has been exploited in the wild.
- A new Action covering **UNC2464** (https://advantage.mandiant.com/actors/UNC2464), an India-based threat cluster that conducts espionage operations targeting the South Asian government sector and Chinese nuclear research entities.
- A new Action covering financially motivated threat cluster **UNC6240** (https://advantage.mandiant.com/actors/UNC6240), responsible for extortion operations branded under the ShinyHunters name and utilizing **SHINYSPIDER** (https://advantage.mandiant.com/malware/SHINYSPIDER).
- A new Action covering **UNC6396** (https://advantage.mandiant.com/actors/UNC6396), a China-nexus threat group suspected of espionage targeting government organizations in Southeast Asia, observed deploying **SHYROOSTER** (https://advantage.mandiant.com/malware/SHYROOSTER) and **TACKYPASTA** (https://advantage.mandiant.com/malware/TACKYPASTA).
- New Actions covering **UNC3569** (https://advantage.mandiant.com/actors/UNC3569), a suspected China-nexus cyber actor of unknown motivation, reportedly deploying ransomware and using various malware.
- New Actions describing **Campaign 26-056** (https://advantage.mandiant.com/campaigns/CAMP.26.056), a financially motivated **UNC6801** (https://advantage.mandiant.com/actors/UNC6801) campaign delivering **REMCOS** (https://advantage.mandiant.com/malware/REMCOS) via multi-stage loaders.
- New Actions demonstrating **Campaign 26-036** (https://advantage.mandiant.com/campaigns/CAMP.26.036), a supply chain campaign by **UNC6780** (https://advantage.mandiant.com/actors/UNC6780) targeting cloud credential theft and exfiltration via compromised Trivy and LiteLLM software.

New Actions

A total of 83 Actions have been added to the content baseline with this update. This includes 61 Network Actions, 7 Host CLI Actions, and 15 Protected Theater Actions. All Actions in this release are tagged using the MITRE ATT&CK v17.1 framework.

Network Actions

VID	Name	Tags
A108-672	Command and Control - CVE-2026-0300, Exploitation, Variant #1	ATT&CK:Command and Control,ATT&CK:T1071.001,CVE-2026-0300,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-673	Command and Control - UNC3569, GRAYRABBIT, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:Execution,ATT&CK:M1026,ATT&CK:M1031,ATT&CK:M1038,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1049,ATT&CK:T1059.001,ATT&CK:T1071.001,ATT&CK:T1105,Actor:UNC3569,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GRAYRABBIT,NIST:CM-11,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-675	Command and Control - UNC6849, CHALKWIRE, VIDAR, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,Actor:UNC6849,CAMP.26.059,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:CHALKWIRE,Malware:VIDAR,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-676	Command and Control - UNC6849, CHALKWIRE, VIDAR, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,ATT&CK:T1132.001,Actor:UNC6849,CAMP.26.059,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CHALKWIRE,Malware:VIDAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-677	Command and Control - UNC6849, NEONSLIDE, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6849,CAMP.26.059,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:NEONSLIDE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-685	Malicious File Transfer - DUSTMAKER, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.060,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-686	Malicious File Transfer - DUSTMAKER, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.060,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-687	Malicious File Transfer - HELLCAT, HELLCAT.GO, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HELLCAT,Malware:HELLCAT.GO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-688	Malicious File Transfer - UNC3569, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3569,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-689	Malicious File Transfer - UNC3569, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3569,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-690	Malicious File Transfer - UNC3569, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3569,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-691	Malicious File Transfer - UNC3569, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3569,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-692	Malicious File Transfer - UNC3569, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3569,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-693	Malicious File Transfer - UNC3569, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3569,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-694	Malicious File Transfer - UNC3569, GRAYRABBIT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3569,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GRAYRABBIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-695	Malicious File Transfer - UNC3569, GRAYRABBIT, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3569,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GRAYRABBIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-696	Malicious File Transfer - UNC3569, METASPLOIT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3569,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:METASPLOIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-697	Malicious File Transfer - UNC3569, METASPLOIT, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3569,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:METASPLOIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-698	Malicious File Transfer - UNC6240, SHINYSPIDER, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6240,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHINYSPIDER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-699	Malicious File Transfer - UNC6396, SHYROOSTER, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6396,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHYROOSTER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-700	Malicious File Transfer - UNC6396, SHYROOSTER, TACKYPASTA, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6396,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHYROOSTER,Malware:TACKYPASTA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-701	Malicious File Transfer - UNC6731, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6731,CAMP.26.058,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-702	Malicious File Transfer - UNC6780, ADAPTAGENT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ADAPTAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-703	Malicious File Transfer - UNC6780, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-704	Malicious File Transfer - UNC6780, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-705	Malicious File Transfer - UNC6780, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-706	Malicious File Transfer - UNC6780, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-707	Malicious File Transfer - UNC6780, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-708	Malicious File Transfer - UNC6780, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,CAMP.26.052,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-709	Malicious File Transfer - UNC6780, MOONBEAM, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MOONBEAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-710	Malicious File Transfer - UNC6780, MOONBEAM, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MOONBEAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-711	Malicious File Transfer - UNC6780, MOONBEAM, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MOONBEAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-712	Malicious File Transfer - UNC6780, QUICKSTEP, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:QUICKSTEP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-713	Malicious File Transfer - UNC6780, QUICKSTEP, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:QUICKSTEP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-714	Malicious File Transfer - UNC6780, QUICKSTEP, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:QUICKSTEP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-715	Malicious File Transfer - UNC6780, QUICKSTEP, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:QUICKSTEP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-716	Malicious File Transfer - UNC6780, SANDCLOCK, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDCLOCK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-717	Malicious File Transfer - UNC6780, SANDCLOCK, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,CAMP.26.036,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDCLOCK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-718	Malicious File Transfer - UNC6780, SANDCLOCK, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,CAMP.26.036,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDCLOCK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-719	Malicious File Transfer - UNC6780, SANDCLOCK, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,CAMP.26.036,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDCLOCK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-720	Malicious File Transfer - UNC6780, SANDCLOCK, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDCLOCK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-721	Malicious File Transfer - UNC6780, SANDCLOCK, SANDCLOCK.JS, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDCLOCK,Malware:SANDCLOCK.JS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-722	Malicious File Transfer - UNC6801, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6801,CAMP.26.056,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-723	Malicious File Transfer - UNC6801, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6801,CAMP.26.056,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-724	Malicious File Transfer - UNC6801, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6801,CAMP.26.056,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-725	Malicious File Transfer - UNC6801, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6801,CAMP.26.056,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-726	Malicious File Transfer - UNC6801, REMCOS, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6801,CAMP.26.056,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-727	Malicious File Transfer - UNC6801, REMCOS, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6801,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-728	Malicious File Transfer - UNC6841, DRYROT, DRYROT.V2, THICKSHELL, ZAPCAT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6841,CAMP.26.053,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DRYROT,Malware:DRYROT.V2,Malware:THICKSHELL,Malware:ZAPCAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-729	Malicious File Transfer - UNC6841, SIDEFOX, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6841,CAMP.26.053,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SIDEFOX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-730	Malicious File Transfer - UNC6841, ZAPCAT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6841,CAMP.26.053,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ZAPCAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-731	Malicious File Transfer - UNC6847, ADAPTAGENT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6847,CAMP.26.057,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ADAPTAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-732	Malicious File Transfer - UNC6847, ADAPTAGENT, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6847,CAMP.26.057,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ADAPTAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-733	Malicious File Transfer - UNC6849, VIDAR, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6849,CAMP.26.059,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VIDAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-734	Malicious File Transfer - UNC6863, BADFALL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6863,CAMP.26.054,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADFALL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-735	Malicious File Transfer - UNC6863, BADFALL, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6863,CAMP.26.054,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADFALL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-736	Malicious File Transfer - UNC6863, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6863,CAMP.26.054,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-737	Malicious File Transfer - UNC6863, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6863,CAMP.26.054,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-738	Malicious File Transfer - UNC6863, SLICKDEMON, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6863,CAMP.26.054,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-739	Malicious File Transfer - UNC6863, SLICKDEMON, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6863,CAMP.26.054,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-740	Malicious File Transfer - UNC6863, SLICKDEMON, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6863,CAMP.26.054,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

Host CLI Actions

VID	Name	Tags
A108-678	Host CLI - Reconnaissance Via Trivy Vulnerability Scanner, Variant #1	ATT&CK:M1056,ATT&CK:Reconnaissance,ATT&CK:T1592.002,Actor:UNC6780,Control:Endpoint,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-679	Host CLI - Search For Aws Credentials In Files, Variant #1	ATT&CK:Credential Access,ATT&CK:M1017,ATT&CK:M1022,ATT&CK:M1027,ATT&CK:M1047,ATT&CK:T1552.001,Actor:UNC6780,CWE:259,CWE:522,CWE:798,Control:Endpoint,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-680	Host CLI - Search For Credentials In Files Using Grep, Variant #1	ATT&CK:Credential Access,ATT&CK:M1017,ATT&CK:M1022,ATT&CK:M1027,ATT&CK:M1047,ATT&CK:T1552.001,Actor:UNC6780,CWE:259,CWE:522,CWE:798,Control:Endpoint,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-681	Host CLI - UNC6780, Discover Cloud Credentials In Environment, Variant #1	ATT&CK:Credential Access,ATT&CK:M1015,ATT&CK:M1017,ATT&CK:M1022,ATT&CK:M1026,ATT&CK:M1027,ATT&CK:M1028,ATT&CK:M1030,ATT&CK:M1035,ATT&CK:M1037,ATT&CK:M1041,ATT&CK:M1042,ATT&CK:M1047,ATT&CK:M1051,ATT&CK:T1552,Actor:UNC6780,Control:Endpoint,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-682	Host CLI - UNC6780, Steal Shell History, Variant #1	ATT&CK:Collection,ATT&CK:M1057,ATT&CK:T1005,Actor:UNC6780,CWE:200,Control:Endpoint,NIST:AC-23,NIST:AC-4,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-683	Host CLI - UNC6841, In Memory C# Compilation, Variant #1	ATT&CK:Defense Evasion,ATT&CK:T1027.004,Actor:UNC6841,CAMP.26.053,Control:Endpoint,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-684	Host CLI - UNC6857, Hiding User Account From Logon Screen, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1028,ATT&CK:T1564.002,Actor:UNC6857,CAMP.26.062,Control:Endpoint,NIST:AC-2,NIST:IA-2,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted

Protected Theater Actions

VID	Name	Tags
A108-741	Protected Theater - BLACKWIDOW, Execute Obfuscated Powershell Download Cradle, Variant #1	ATT&CK:Execution,ATT&CK:M1026,ATT&CK:M1038,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1049,ATT&CK:T1059.001,Actor:UNC6844,CAMP.26.053,CAMP.26.055,Control:Endpoint,Malware:BLACKWIDOW,NIST:CM-11,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-742	Protected Theater - Create Malicious Service For Credential Manipulation, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC6857,CAMP.26.062,CWE:284,Control:Endpoint,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-743	Protected Theater - Executes Autoit C2 Beacon, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,CAMP.26.056,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-744	Protected Theater - MOONLEAF, Hijack Execution Via Npm Postinstall Script, Variant #1	ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1026,ATT&CK:M1028,ATT&CK:M1035,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1047,ATT&CK:M1051,ATT&CK:M1052,ATT&CK:M1054,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1546,Actor:UNC6780,Control:Endpoint,Malware:MOONLEAF,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-745	Protected Theater - Persistence Via Systemd User Service, Variant #1	ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1026,ATT&CK:M1033,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.002,Actor:UNC6780,Control:Endpoint,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-746	Protected Theater - UNC2464, Persistence, Variant #1	ATT&CK:Execution,ATT&CK:M1018,ATT&CK:M1026,ATT&CK:M1028,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1053.005,Actor:UNC2464,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A108-747	Protected Theater - UNC3569, GRAYRABBIT, Beacons To A C2 Domain, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC3569,Control:Endpoint,Malware:GRAYRABBIT,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-748	Protected Theater - UNC3569, GRAYRABBIT, Execute Payload With Input Redirection, Variant #1	ATT&CK:Execution,ATT&CK:M1038,ATT&CK:T1059.003,Actor:UNC3569,Control:Endpoint,Malware:GRAYRABBIT,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-749	Protected Theater - UNC3569, METASPLOIT, Amd64.Elf C2 Beacon, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC3569,Control:Endpoint,Malware:METASPLOIT,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-750	Protected Theater - UNC3569, METASPLOIT, Executes Linux Stager, Variant #1	ATT&CK:Execution,ATT&CK:M1038,ATT&CK:T1059.004,Actor:UNC3569,Control:Endpoint,Malware:METASPLOIT,NIST:CM-11,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-751	Protected Theater - UNC3569, Powershell On The Fly Compilation, Variant #1	ATT&CK:Execution,ATT&CK:M1026,ATT&CK:M1038,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1049,ATT&CK:T1059.001,Actor:UNC3569,Control:Endpoint,NIST:CM-11,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-752	Protected Theater - UNC6780, ADAPTAGENT, Execution Leading To C2 Connection, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6780,Control:Endpoint,Malware:ADAPTAGENT,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-753	Protected Theater - UNC6780, SANDCLOCK, Execute Malware For Data Exfiltration, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6780,Control:Endpoint,Malware:SANDCLOCK,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-754	Protected Theater - UNC6780, SANDCLOCK.SH, Exfiltrates Data Via Dns, Variant #1	ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,Actor:UNC6780,Control:Endpoint,Malware:SANDCLOCK.SH,NIST:AC-4,NIST:CM-7,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-755	Protected Theater - UNC6801, REMCOS, Execute Payload, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6801,CAMP.26.056,Control:Endpoint,Malware:REMCOS,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted

New Files

A total of 61 new files have been added to the File Library with this update. This includes 61 malicious files and 0 non-malicious files.

Malicious Files

File MD5	Tags
04240dd0ea8f3567078e786ab3125808	Group:Validation
05bacbe163ef0393c2416cbd05e45e74	Malware:SANDCLOCK.JS,Group:Validation
0c32c727569c2387a95ac533dace4255	Malware:GRAYRABBIT,Group:Validation,Malware_Type:BACKDOOR
0c7a919b3b47df95425ddb7b0cfce29e	Malware:QUICKSTEP,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
151699d7b7ffd59c1efa417c7503fe8d	Malware_Type:BACKDOOR,Malware:ADAPTAGENT,Group:Validation
185ba25adc361708db58b364a57efaea	Group:Validation,Malware:REMCOS,Malware_Type:BACKDOOR
188d8592f393ce45f7273102f02efee1	Group:Validation
1d9c8de1a6317a9f633b85b78d6e42a8	Group:Validation,Malware:VIDAR,Malware_Type:DROPPER_MEMORY_ONLY
29fa05b128d3f21ba3b7ba84f71fa024	Group:Validation
2b3875b6b7913a5a61e2acccb4fb8ca9	Malware_Type:RANSOMWARE,Malware:SHINYSPIDER,Group:Validation
2c00a9ae4d98736d883d0cad6ca289bb	Group:Validation
36fe1825a7773b8f3eabadbdad57aece	Malware:ZAPCAT,Malware_Type:BACKDOOR,Group:Validation
3ae21dd1eee0963bdc1337e83ef1719f	Malware:GRAYRABBIT,Group:Validation
410514a0aaaa04a4438017373ce4c462	Group:Validation,Malware:SIDEFOX
46e7a5c4cf645b77f24023eef873f56f	Malware:QUICKSTEP,Malware_Type:DROPPER,Group:Validation
46f62ef74369402146d5fbb7f41b6bb1	Group:Validation
517fcdeb7e4e6be4a37ac2bc70e975ee	Group:Validation
55405de62427ac56106f0fdb1c33dedd	Group:Validation,Malware:QUICKSTEP
55fd8864d00b54eef23f90746b160f27	Malware:GRAYRABBIT,Group:Validation,Malware_Type:BACKDOOR
599a186de45023bddfb37ba52d69dbf5	Malware_Type:DOWNLOADER,Group:Validation
5d5778d99b633f688832ba80f1ed80a7	Group:Validation
6248b61890492fdd04911ef1623c5a63	Group:Validation
6c9da8de6797d4a446d962d5f3f0c22c	Malware:SANDCLOCK,Group:Validation
7050a0b2d59e63d84eecb5465a7b9350	Group:Validation
707356186af8a147e45c8033baabc8d1	Malware:METASPLOIT,Group:Validation
718c13820bff309925b5b629bbb5da2c	Malware_Type:EXPLOIT,Malware:MOONBEAM,Group:Validation
73df2a54e8b0170078e0f3ab5707d85b	Malware:SLICKDEMON,Malware_Type:DATA_MINER,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
74053a07e633d9ffa9479a9f070d861a	Group:Validation
7646a872455dab186dc9de17f7ef0340	Malware_Type:DROPPER,Group:Validation
7a9335ed73fab541f5a414ec15e334d5	Malware:BADFALL,Malware_Type:LAUNCHER,Group:Validation
7ab5ecb2acce7d22fcf99ca9429f5a0f	Malware:METASPLOIT,Group:Validation
7cac57b2d328bd814009772dd1eda429	Malware:SANDCLOCK,Group:Validation
8232e0c75f4ddc01cf846646f484ab43	Malware:SHYROOSTER,Malware_Type:BACKDOOR,Malware:TACKYPASTA,Group:Validation
833fd59ebe66a4449982c6d18db656b4	Malware:DUSTMAKER,Group:Validation
8bfefb76454efe404359831d4fe7137c	Malware:MOONBEAM,Malware_Type:EXPLOIT,Group:Validation
9635b50b5a3325ec0ef5f23f0e9cea7c	Malware_Type:BACKDOOR,Malware:BADFALL,Group:Validation
986a8af4d0b5ea68e1949de5fefdfbf2	Malware:QUICKSTEP,Group:Validation
9c51988ffc22eb6d22bbde0185fdf76c	Group:Validation
9c9aa6a37c8f5d2928c48422cc449921	Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation,Malware:THICKSHELL,Malware:ZAPCAT,Malware:DRYROT.V2
9e837f0b9e8037b06256e2ec4291f757	Malware_Type:DOWNLOADER,Group:Validation
9f00f9f7b43b93acc9e478017b93b001	Group:Validation
9f1345519be6b978867e2e7dccc2db62	Malware:GRAYRABBIT,Group:Validation,Malware_Type:LAUNCHER
a14f47e751c567f0d80d3d03d57dbd86	Malware:REMCOS,Malware_Type:BACKDOOR,Group:Validation
a363c1529033fb6017985ce07ab0ad57	Malware:SHYROOSTER,Group:Validation,Malware_Type:LAUNCHER
af90352dcdeb09d4a19ed975923ed038	Group:Validation
b1c6036b046bcf8c80601742ebcc61b0	Malware_Type:DOWNLOADER,Group:Validation
b676c0703f8e4d6a198aa370ca4f5405	Malware_Type:BACKDOOR,Malware:SANDCLOCK,Group:Validation
b82e54923f7e440664d2d75bd31588ca	Malware:DUSTMAKER,Group:Validation
be53eb553067f1f8d031843dedbd604c	Malware:HELLCAT.GO,Malware_Type:RANSOMWARE,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
cc96b513eff7c4a653e23e7c41f7bbd5	Group:Validation
cde4951bee7e28ac8a29d33d34a41ae5	Group:Validation,Malware:SANDCLOCK
d07b92d021dd25daf73de1d706634cf2	Malware_Type:BACKDOOR,Malware:ADAPTAGENT,Group:Validation
d47de3772f2d61a043e7047431ef4cf4	Group:Validation,Malware:DUSTMAKER
d528effabbd9cd66aaa11bc8777bb110	Malware:ADAPTAGENT,Malware_Type:BACKDOOR,Group:Validation
d5e2932a0a4cc5b74521a684d00be40d	Malware_Type:DROPPER,Group:Validation
dca6c0722219f684ac7e971f843599fb	Group:Validation
de913f86e934df1d6e7f96a0c365c728	Malware:SANDCLOCK,Group:Validation
df43394b926e609e6ad020b157b151a1	Malware_Type:EXPLOIT,Malware:MOONBEAM,Group:Validation
f209fbca69e9a25c2cdbfbd9c973ba9f	Malware:SLICKDEMON,Malware_Type:DATA_MINER,Group:Validation
f2bd550773af344661689e259ffb97ed	Malware:SLICKDEMON,Malware_Type:DATA_MINER,Group:Validation
f3479b029ac96c4043d22e2e44a62a9d	Group:Validation

Updated Content

Changes include improved consistency in execution, description details, and tags. For more information, see **Content pack downloads (https://docs.mandiant.com/home/msv-content-packs)** (requires sign in).

Supported Operating Systems (OS) and Platforms

VRT used the following environments to test the Validation content included in this update. Each Action is assigned OS/Platform Tags, which you can see when viewing the Action in the Action Library. These tags indicate which environments we expect the Action to run successfully on and are the environments the Actions were tested on.

Mandiant Security Validation Platform

System	Build Number / Version
Director	4.14.4.1-51
Actor	4.12.4.1-8

Network Actions

OS/Platform	Common Platform Enumeration (CPE)
Linux: CentOS	cpe:2.3:o:redhat:enterprise_linux:7.8:*:*:en-us:*:*:x64

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.