Mandiant

VHR20260506 - MAY 6, 2026

The Mandiant Intelligence Validation Research Team (VRT) has published VHR20260506 - 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

- 273 Actions added
- 111 Files added
- 4 Actions retired

Release Highlights

- New Actions demonstrating **Campaign 26-018** (https://advantage.mandiant.com/campaigns/CAMP.26.018), exploiting **CVE-2026-20127** (https://advantage.mandiant.com/vulnerabilities/CVE-2026-20127) and **CVE-2022-20775** (https://advantage.mandiant.com/vulnerabilities/CVE-2022-20775) in Cisco Catalyst SD-WAN devices.
- New Actions covering **Campaign 26-020** (https://advantage.mandiant.com/campaigns/CAMP.26.020), which involves a threat actor deploying **WINDSTRIKE** (https://advantage.mandiant.com/malware/WINDSTRIKE) malware via trojanized software to establish persistence and evade defenses.
- New Actions demonstrating **Campaign 26-023** (https://advantage.mandiant.com/campaigns/CAMP.26.023), a campaign by **UNC6740** (https://advantage.mandiant.com/actors/UNC6740) deploying **DINODANCE** (https://advantage.mandiant.com/malware/DINODANCE) malware using trojanized installers and Deno Runtime for in-memory execution.
- New Actions demonstrating **Campaign 26-028** (https://advantage.mandiant.com/campaigns/CAMP.26.028), a campaign by **APT42** (https://advantage.mandiant.com/actors/APT42) using phishing kits with fake media lures for credential harvesting and deploying **TAMECAT** (https://advantage.mandiant.com/malware/TAMECAT) and **POWERPUG** (https://advantage.mandiant.com/malware/POWERPUG) malware.
- New Actions demonstrating **Campaign 26-015** (https://advantage.mandiant.com/campaigns/CAMP.26.015), a campaign involving actor **UNC6674** (https://advantage.mandiant.com/actors/UNC6674) leveraging Windows batch scripts to deliver a shellcode injector tool, including **VALLEYRAT** (https://advantage.mandiant.com/malware/VALLEYRAT).
- New Actions demonstrating **Campaign 26-029** (https://advantage.mandiant.com/campaigns/CAMP.26.029), a campaign by **UNC3313** (https://advantage.mandiant.com/actors/UNC3313) and **UNC5667** (https://advantage.mandiant.com/actors/UNC5667) targeting multiple industry verticals globally with custom backdoors and legitimate remote access tools.
- New Actions demonstrating **Campaign 26-032** (https://advantage.mandiant.com/campaigns/CAMP.26.032), a financially motivated campaign by **UNC6769** (https://advantage.mandiant.com/actors/UNC6769) using MSHTA and obfuscated PowerShell to deploy **AMATERASTEALER** (https://advantage.mandiant.com/malware/AMATERASTEALER).
- A new Action covering **Campaign 26-024** (https://advantage.mandiant.com/campaigns/CAMP.26.024), a suspected Iranian threat group **UNC6729** (https://advantage.mandiant.com/actors/UNC6729) campaign targeting Israeli citizens with **PANICPOACH** (https://advantage.mandiant.com/malware/PANICPOACH) Android Malware.
- A new Action covering **Campaign 26-034** (https://advantage.mandiant.com/campaigns/CAMP.26.034), a campaign exploiting **CVE-2026-1281** (https://advantage.mandiant.com/vulnerabilities/CVE-2026-1281) and **CVE-2026-1340** (https://advantage.mandiant.com/vulnerabilities/CVE-2026-1340) in Ivanti EPMM for initial access by a threat actor of unknown motivations.
- A new Action covering **Campaign 26-035** (https://advantage.mandiant.com/campaigns/CAMP.26.035), concerning an unknown actor leveraging **CVE-2026-1731** (https://advantage.mandiant.com/vulnerabilities/CVE-2026-1731) for initial access via BeyondTrust's Remote Support software.
- New Actions demonstrating **Campaign 26-041** (https://advantage.mandiant.com/campaigns/CAMP.26.041), a suspected

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

DPRK threat actor campaign leveraging malicious GitHub repositories to deliver **BEAVERTAIL** (https://advantage.mandiant.com/malware/BEAVERTAIL).

- New Actions covering **Campaign 26-039** (https://advantage.mandiant.com/campaigns/CAMP.26.039) by **UNC6765** (https://advantage.mandiant.com/actors/UNC6765), an actor of unknown motivations, leveraging social engineering, living-off-the-land tools such as **ANYDESK** (https://advantage.mandiant.com/malware/ANYDESK) and **CURL** (https://advantage.mandiant.com/malware/CURL), and SSH reverse tunnels for persistence and execution.
- A new Action demonstrating **Campaign 26-043** (https://advantage.mandiant.com/campaigns/CAMP.26.043), a financial gain actor **UNC6767** (https://advantage.mandiant.com/actors/UNC6767) campaign leveraging **CVE-2025-55182** (https://advantage.mandiant.com/vulnerabilities/CVE-2025-55182) and deploying **NETSUPPORT** (https://advantage.mandiant.com/malware/NETSUPPORT).
- New Actions demonstrating **Campaign 26-047** (https://advantage.mandiant.com/campaigns/CAMP.26.047) where an actor of unknown motivations exploits **CVE-2026-1731** (https://advantage.mandiant.com/vulnerabilities/CVE-2026-1731) to deploy **SPARKRAT** (https://advantage.mandiant.com/malware/SPARKRAT).
- New Actions covering **Campaign 26-042** (https://advantage.mandiant.com/campaigns/CAMP.26.042), a North Korea-nexus actor **UNC1069** (https://advantage.mandiant.com/actors/UNC1069) supply chain attack deploying **SILKBELL** (https://advantage.mandiant.com/malware/SILKBELL) and **WAVESHAPER** (https://advantage.mandiant.com/malware/WAVESHAPER.V2.MACHO) backdoor variants.
- A new Action covers **Campaign 26-026** (https://advantage.mandiant.com/campaigns/CAMP.26.026) by **UNC6724** (https://advantage.mandiant.com/actors/UNC6724) leveraging CLICKFIX for initial access, followed by MSHTA commands and PowerShell for payload delivery, including **BEACON** (https://advantage.mandiant.com/malware/BEACON).
- New Actions demonstrating **Campaign 26-050** (https://advantage.mandiant.com/campaigns/CAMP.26.050), an unknown threat group **UNC6781** (https://advantage.mandiant.com/actors/UNC6781) campaign targeting US Universities with trojanized NSIS installers, hidden Python environments, and **NETSUPPORT** (https://advantage.mandiant.com/malware/NETSUPPORT) RAT deployments.
- A new Action demonstrating **Campaign 26-049** (https://advantage.mandiant.com/campaigns/CAMP.26.049), a Brazil-nexus threat group **UNC5669** (https://advantage.mandiant.com/actors/UNC5669) campaign executing multi-vector breaches and deploying **XWORM** (https://advantage.mandiant.com/malware/XWORM).
- New Actions demonstrating **Campaign 26-051** (https://advantage.mandiant.com/campaigns/CAMP.26.051), a suspected espionage threat group **UNC6723** (https://advantage.mandiant.com/actors/UNC6723) weaponizing **RCLONE** (https://advantage.mandiant.com/malware/RCLONE) to exfil sensitive docs and Telegram data to Mega accounts.
- A new Action covering **CVE-2026-34621** (https://advantage.mandiant.com/vulnerabilities/CVE-2026-34621), an Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') vulnerability that allows a remote attacker to execute arbitrary code.
- A new Action covering **Campaign 26-037** (https://advantage.mandiant.com/campaigns/CAMP.26.037), a campaign by **UNC6760** (https://advantage.mandiant.com/actors/UNC6760) distributing the **TIREPATCH** (https://advantage.mandiant.com/malware/TIREPATCH) downloader via FAKETREFF and ClickFix infection vectors.

New Actions

A total of 273 Actions have been added to the content baseline with this update. This includes 152 Network Actions, 10 Host CLI Actions, and 111 Protected Theater Actions. All Actions in this release are tagged using the MITRE ATT&CK v17.1 framework.

Network Actions

VID	Name	Tags

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-397	Command and Control - APT42, TAMECAT, Tasking, Variant #2	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:APT42,CAMP.26.028,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TAMECAT,NIST:CM-11,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-398	Command and Control - APT42, Telegram, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:APT42,CAMP.26.028,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-399	Command and Control - CVE-2026-34621 Loader, Environment Fingerprinting and Payload Delivery, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,CVE-2026-34621,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-400	Command and Control - CVE-2026-34621 Loader, Payload Request, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,CVE-2026-34621,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-401	Command and Control - CVE-2026-34621 Loader, Payload Request, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,CVE-2026-34621,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-402	Command and Control - LIGHTPHOENIX, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1132.001,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:LIGHTPHOENIX,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-403	Command and Control - LIGHTPHOENIX, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:Defense Evasion,ATT&CK:M1031,ATT&CK:M1040,ATT&CK:M1049,ATT&CK:T1027,ATT&CK:T1071.001,CAMP.26.029,CWE:173,CWE:20,CWE:697,CWE:74,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTPHOENIX,NIST:AC-4,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-404	Command and Control - LIGHTPHOENIX, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1030,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1571,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTPHOENIX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-405	Command and Control - MIMIKATZ, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:Discovery,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1082,CAMP.26.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:MIMIKATZ,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-406	Command and Control - MIMIKATZ, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,CAMP.26.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:MIMIKATZ,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-407	Command and Control - UNC1069, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:Discovery,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,ATT&CK:T1083,Actor:UNC1069,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-408	Command and Control - UNC1069, Exfiltration, Variant #2	ATT&CK:Collection,ATT&CK:Command and Control,ATT&CK:Discovery,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1005,ATT&CK:T1041,ATT&CK:T1071.001,ATT&CK:T1083,Actor:UNC1069,CAMP.26.042,CWE:200,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:AC-23,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-409	Command and Control - UNC1069, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1030,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1571,Actor:UNC1069,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-410	Command and Control - UNC3313, ATERA, Check-In, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:M1037,ATT&CK:M1038,ATT&CK:T1071.001,ATT&CK:T1219,Actor:UNC3313,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:AC-17,NIST:AC-3,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-411	Command and Control - UNC3313, ATERA, Check-In, Variant #3	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:M1037,ATT&CK:M1038,ATT&CK:T1071.001,ATT&CK:T1102,ATT&CK:T1219,Actor:UNC3313,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:AC-17,NIST:AC-3,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-412	Command and Control - UNC3313, ATERA, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,Actor:UNC3313,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-413	Command and Control - UNC3313, ATERA, Tasking, Variant #2	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,ATT&CK:T1105,Actor:UNC3313,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-414	Command and Control - UNC3313, MIRADORE, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573,Actor:UNC3313,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:MIRADORE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-415	Command and Control - UNC3313, MIRADORE, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC3313,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:MIRADORE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-416	Command and Control - UNC3313, OPENGAZE, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573.001,Actor:UNC3313,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:OPENGAZE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-417	Command and Control - UNC3313, OPENGAZE, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC3313,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:OPENGAZE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-418	Command and Control - UNC3313, SYNCRO, Check-In, Variant #3	ATT&CK:Command and Control,ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:M1026,ATT&CK:M1028,ATT&CK:M1031,ATT&CK:M1039,ATT&CK:M1042,ATT&CK:M1047,ATT&CK:M1054,ATT&CK:T1071.001,ATT&CK:T1562,Actor:UNC3313,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:SYNCRO,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-419	Command and Control - UNC3313, SYNCRO, Communication, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:M1037,ATT&CK:M1038,ATT&CK:T1071.001,ATT&CK:T1105,ATT&CK:T1219,Actor:UNC3313,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SYNCRO,NIST:AC-17,NIST:AC-3,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-420	Command and Control - UNC3313, SYNCRO, Communication, Variant #4	ATT&CK:Command and Control,ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1562.001,Actor:UNC3313,CAMP.26.029,CWE:284,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:SYNCRO,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-421	Command and Control - UNC3313, SYNCRO, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:Discovery,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1082,ATT&CK:T1518.001,Actor:UNC3313,CAMP.26.029,Control:NGFW,Control:Proxy,Malware:SYNCRO,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-422	Command and Control - UNC3313, SYNCRO, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC3313,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SYNCRO,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-423	Command and Control - UNC3313, SYNCRO, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC3313,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SYNCRO,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-424	Command and Control - UNC3313, SYNCRO, Tasking, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC3313,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SYNCRO,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-425	Command and Control - UNC5667, Check-In, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-426	Command and Control - UNC5667, FRONTLOAD, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FRONTLOAD,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-427	Command and Control - UNC5667, LIGHTPHOENIX, Check-In, Variant #3	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:LIGHTPHOENIX,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-428	Command and Control - UNC5667, LIGHTPHOENIX, Registration, Variant #4	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1001,ATT&CK:T1041,ATT&CK:T1071.001,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTPHOENIX,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-429	Command and Control - UNC5667, POTATOWALL, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POTATOWALL,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-430	Command and Control - UNC5667, POTATOWALL, Telegram, Variant #5	ATT&CK:Command and Control,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POTATOWALL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-431	Command and Control - UNC5667, POTATOWALL, Telegram, Variant #6	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POTATOWALL,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-432	Command and Control - UNC5667, POTATOWALL, Telegram, Variant #7	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POTATOWALL,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-433	Command and Control - UNC5667, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1132.001,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-434	Command and Control - UNC5667, RUBBERAXE, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:RUBBERAXE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-435	Command and Control - UNC5667, SOFTMETAL, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SOFTMETAL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-436	Command and Control - UNC6674, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6674,CAMP.26.015,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-437	Command and Control - UNC6674, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,Actor:UNC6674,CAMP.26.015,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-438	Command and Control - UNC6676, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6676,CAMP.26.041,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-439	Command and Control - UNC6676, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6676,CAMP.26.041,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-440	Command and Control - UNC6676, Tasking, Variant #2	ATT&CK:Command and Control,ATT&CK:Execution,ATT&CK:Exfiltration,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:M1042,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1059.007,ATT&CK:T1071.001,ATT&CK:T1105,Actor:UNC6676,CAMP.26.041,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-441	Command and Control - UNC6740, DINODANCE, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6740,CAMP.26.023,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DINODANCE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-442	Command and Control - UNC6740, DINODANCE, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6740,CAMP.26.023,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:DINODANCE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-443	Command and Control - UNC6740, DINODANCE, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:Defense Evasion,ATT&CK:M1031,ATT&CK:M1040,ATT&CK:M1049,ATT&CK:T1027,ATT&CK:T1071.001,ATT&CK:T1105,Actor:UNC6740,CAMP.26.023,CWE:173,CWE:20,CWE:697,CWE:74,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DINODANCE,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-444	Command and Control - UNC6740, DINODANCE, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,Actor:UNC6740,CAMP.26.023,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DINODANCE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-445	Command and Control - UNC6740, DINODANCE, Tasking, Variant #2	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:UNC6740,CAMP.26.023,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DINODANCE,NIST:CM-11,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-446	Command and Control - UNC6753, SPARKRAT, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1030,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1571,Actor:UNC6753,CAMP.26.047,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:SPARKRAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-447	Command and Control - UNC6758, SHADOWRICE, 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:UNC6758,CAMP.26.032,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHADOWRICE,NIST:CM-11,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-458	Malicious File Transfer - APT42, TAMECAT, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,CAMP.26.028,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TAMECAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-459	Malicious File Transfer - APT42, TAMECAT, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,CAMP.26.028,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TAMECAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-460	Malicious File Transfer - APT42, TAMECAT, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,CAMP.26.028,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TAMECAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-461	Malicious File Transfer - APT42, TAMECAT, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,CAMP.26.028,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TAMECAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-462	Malicious File Transfer - CVE-2026-34621 Loader, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CVE-2026-34621,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-463	Malicious File Transfer - MIMIKATZ, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MIMIKATZ,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-464	Malicious File Transfer - REMCOM, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.049,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-465	Malicious File Transfer - UNC1069, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-466	Malicious File Transfer - UNC1069, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-467	Malicious File Transfer - UNC1069, SILKBELL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SILKBELL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-468	Malicious File Transfer - UNC1069, SILKBELL, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SILKBELL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-469	Malicious File Transfer - UNC1069, SILKBELL, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SILKBELL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-470	Malicious File Transfer - UNC1069, SILKBELL, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SILKBELL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-471	Malicious File Transfer - UNC1069, WAVESHAPER, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-472	Malicious File Transfer - UNC1069, WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.MACHO, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.MACHO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-473	Malicious File Transfer - UNC1069, WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.MACHO, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.MACHO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-474	Malicious File Transfer - UNC1069, WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.PS, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.PS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-475	Malicious File Transfer - UNC1069, WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.PS, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.PS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-476	Malicious File Transfer - UNC1069, WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.PS, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.PS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-477	Malicious File Transfer - UNC1069, WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.PS, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.PS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-478	Malicious File Transfer - UNC1069, WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.PY, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.PY,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-479	Malicious File Transfer - UNC1069, WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.PY, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.PY,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-480	Malicious File Transfer - UNC3313, Download, Variant #23	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-481	Malicious File Transfer - UNC5667, DCPHOENIX, PROTONGLOW, SILVERLIME, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DCPHOENIX,Malware:PROTONGLOW,Malware:SILVERLIME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-482	Malicious File Transfer - UNC5667, Download, Variant #29	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-483	Malicious File Transfer - UNC5667, HORSESHOE, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HORSESHOE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-484	Malicious File Transfer - UNC5667, POTATOWALL, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POTATOWALL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-485	Malicious File Transfer - UNC5667, POTATOWALL, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POTATOWALL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-486	Malicious File Transfer - UNC5667, PROTONGLOW, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PROTONGLOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-487	Malicious File Transfer - UNC5667, SOFTMETAL, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,CAMP.26.029,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SOFTMETAL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-488	Malicious File Transfer - UNC5667, STAGEHAND, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:STAGEHAND,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-489	Malicious File Transfer - UNC5669, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,CAMP.26.049,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-490	Malicious File Transfer - UNC5669, REMCOS, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-491	Malicious File Transfer - UNC5669, SCREENCONNECT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SCREENCONNECT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-492	Malicious File Transfer - UNC5669, XWORM, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:XWORM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-493	Malicious File Transfer - UNC5669, XWORM, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:XWORM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-494	Malicious File Transfer - UNC6674, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6674,CAMP.26.015,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-495	Malicious File Transfer - UNC6674, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6674,CAMP.26.015,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-496	Malicious File Transfer - UNC6674, PURERAT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6674,CAMP.26.015,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PURERAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-497	Malicious File Transfer - UNC6676, BEAVERTAIL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6676,CAMP.26.041,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BEAVERTAIL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-498	Malicious File Transfer - UNC6676, BEAVERTAIL, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6676,CAMP.26.041,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BEAVERTAIL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-499	Malicious File Transfer - UNC6676, BEAVERTAIL, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6676,CAMP.26.041,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BEAVERTAIL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-500	Malicious File Transfer - UNC6676, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6676,CAMP.26.041,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
A108-501	Malicious File Transfer - UNC6676, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6676,CAMP.26.041,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-502	Malicious File Transfer - UNC6676, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6676,CAMP.26.041,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-503	Malicious File Transfer - UNC6676, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6676,CAMP.26.041,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-504	Malicious File Transfer - UNC6676, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6676,CAMP.26.041,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-505	Malicious File Transfer - UNC6676, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6676,CAMP.26.041,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-506	Malicious File Transfer - UNC6715, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6715,CAMP.26.020,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-507	Malicious File Transfer - UNC6715, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6715,CAMP.26.020,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-508	Malicious File Transfer - UNC6715, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6715,CAMP.26.020,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
A108-509	Malicious File Transfer - UNC6715, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6715,CAMP.26.020,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-510	Malicious File Transfer - UNC6715, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6715,CAMP.26.020,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-511	Malicious File Transfer - UNC6723, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6723,CAMP.26.051,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-512	Malicious File Transfer - UNC6723, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6723,CAMP.26.051,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-513	Malicious File Transfer - UNC6723, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6723,CAMP.26.051,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-514	Malicious File Transfer - UNC6723, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6723,CAMP.26.051,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-515	Malicious File Transfer - UNC6723, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6723,CAMP.26.051,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-516	Malicious File Transfer - UNC6723, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6723,CAMP.26.051,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
A108-517	Malicious File Transfer - UNC6724, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6724,CAMP.26.026,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-518	Malicious File Transfer - UNC6729, PANICPOACH, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6729,CAMP.26.024,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PANICPOACH,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-519	Malicious File Transfer - UNC6729, PANICPOACH, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6729,CAMP.26.024,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PANICPOACH,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-520	Malicious File Transfer - UNC6740, DINODANCE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6740,CAMP.26.023,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DINODANCE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-521	Malicious File Transfer - UNC6740, DINODANCE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6740,CAMP.26.023,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DINODANCE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-522	Malicious File Transfer - UNC6753, SPARKRAT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6753,CAMP.26.047,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.004,Malware:SPARKRAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-523	Malicious File Transfer - UNC6754, TIREPATCH, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6754,CAMP.26.037,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TIREPATCH,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-524	Malicious File Transfer - UNC6758, AMATERASTEALER, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6758,CAMP.26.032,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:AMATERASTEALER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-525	Malicious File Transfer - UNC6758, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6758,CAMP.26.032,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-526	Malicious File Transfer - UNC6758, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6758,CAMP.26.032,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-527	Malicious File Transfer - UNC6758, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6758,CAMP.26.032,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-528	Malicious File Transfer - UNC6780, QUICKSTEP, Download, Variant #1	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
A108-529	Malicious File Transfer - UNC6780, SANDCLOCK, Download, Variant #1	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
A108-530	Malicious File Transfer - UNC6780, SANDCLOCK, Download, Variant #2	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
A108-531	Malicious File Transfer - UNC6780, SANDCLOCK, Download, Variant #3	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
A108-532	Malicious File Transfer - UNC6780, SANDCLOCK, Download, Variant #4	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
A108-533	Malicious File Transfer - UNC6780, SANDCLOCK, SANDCLOCK.SH, Download, Variant #1	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,Malware:SANDCLOCK.SH,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-534	Malicious File Transfer - UNC6781, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6781,CAMP.26.050,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-535	Malicious File Transfer - UNC6781, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6781,CAMP.26.050,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-536	Malicious File Transfer - UNC6781, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6781,CAMP.26.050,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-537	Malicious File Transfer - VALLEYRAT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.015,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VALLEYRAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-538	Malicious File Transfer - WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.MACHO, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.MACHO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-539	Malicious File Transfer - WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.MACHO, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.MACHO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-540	Malicious File Transfer - WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.MACHO, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.MACHO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-541	Malicious File Transfer - WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.MACHO, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.MACHO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-542	Malicious File Transfer - WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.MACHO, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.MACHO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-543	Malicious File Transfer - WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.MACHO, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.MACHO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-544	Malicious File Transfer - WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.MACHO, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.MACHO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-545	Malicious File Transfer - WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.MACHO, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.MACHO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-546	Malicious File Transfer - WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.PS, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.PS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-547	Malicious File Transfer - WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.PS, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.PS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-548	Malicious File Transfer - WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.PS, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.PS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-549	Malicious File Transfer - WAVESHAPER, WAVESHAPER.V2, WAVESHAPER.V2.PY, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WAVESHAPER,Malware:WAVESHAPER.V2,Malware:WAVESHAPER.V2.PY,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-550	Phishing Email - Malicious Attachment, APT42, TAMECAT, Variant #1	ATT&CK:Initial Access,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:M1049,ATT&CK:M1054,ATT&CK:T1566.001,Actor:APT42,CAMP.26.028,Control:Email,Malware:TAMECAT,NIST:CM-7,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-551	Phishing Email - Malicious Attachment, UNC6729, PANICPOACH, Variant #1	ATT&CK:Initial Access,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:M1049,ATT&CK:M1054,ATT&CK:T1566.001,Actor:UNC6729,CAMP.26.024,Control:Email,Malware:PANICPOACH,NIST:CM-7,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-552	Phishing Email - Malicious Attachment, Variant #1	ATT&CK:Initial Access,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:M1049,ATT&CK:M1054,ATT&CK:T1566.001,CAMP.26.029,Control:Email,NIST:CM-7,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-553	Phishing Email - Malicious Link, UNC3313, ATERA, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC3313,CAMP.26.029,Control:Email,Malware:ATERA,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-554	Phishing Email - Malicious Link, UNC3313, SYNCRO, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC3313,CAMP.26.029,Control:Email,Malware:SYNCRO,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-555	Phishing Email - Malicious Link, UNC5667, DARKFLIP, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC5667,Control:Email,Malware:DARKFLIP,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-556	Phishing Email - Malicious Link, UNC5667, Variant #2	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC5667,CAMP.26.029,Control:Email,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-557	Phishing Email - Malicious Link, UNC5970, Variant #2	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC5970,Control:Email,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-558	Phishing Email - Malicious Link, UNC6729, Variant #2	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC6729,CAMP.26.024,Control:Email,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted

Host CLI Actions

VID	Name	Tags
A108-448	Host CLI - APT42, TAMECAT, Clear Run History, Variant #1	ATT&CK:Defense Evasion,ATT&CK:T1070.004,Actor:APT42,CAMP.26.032,Control:Endpoint,Malware:TAMECAT,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-449	Host CLI - APT42, TAMECAT, Enumerate System Information, Variant #1	ATT&CK:Discovery,ATT&CK:T1082,Actor:APT42,CAMP.26.028,Control:Endpoint,Malware:TAMECAT,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-450	Host CLI - Execute Perl Script From Stdin, Variant #1	ATT&CK:Execution,ATT&CK:M1038,ATT&CK:T1059.004,CAMP.26.047,Control:Endpoint,NIST:CM-11,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-451	Host CLI - Executes An Executable Masquerading As A Log File, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1017,ATT&CK:M1022,ATT&CK:M1028,ATT&CK:M1038,ATT&CK:M1045,ATT&CK:T1036,CAMP.26.029,CWE:706,Control:Endpoint,NIST:AC-4,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A108-452	Host CLI - Set Full Control Permissions On Directory With Icacls, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1026,ATT&CK:T1222.001,CAMP.26.049,Control:Endpoint,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-453	Host CLI - Store Base64 Data In Registry Value, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1024,ATT&CK:Persistence,ATT&CK:T1112,CAMP.26.039,CWE:15,CWE:732,Control:Endpoint,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-454	Host CLI - UNC6674, PURERAT, VALLEYRAT, Establishes Persistence Via Registry Run Key, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC6674,CAMP.26.015,Control:Endpoint,Malware:PURERAT,Malware:VALLEYRAT,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-455	Host CLI - UNC6721, TURTLESHELL, Dynamic Victim Id Generation, Variant #1	ATT&CK:Discovery,ATT&CK:T1082,Actor:UNC6721,CAMP.26.033,Control:Endpoint,Malware:TURTLESHELL,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-456	Host CLI - UNC6745, Create Hidden Web Shell, Variant #1	ATT&CK:M1018,ATT&CK:M1042,ATT&CK:Persistence,ATT&CK:T1505.003,Actor:UNC6745,CAMP.26.035,CWE:287,CWE:553,Control:Endpoint,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-457	Host CLI - XWORM, Persistence Via Startup Folder Lnk File, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,CAMP.26.049,Control:Endpoint,Malware:XWORM,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
A108-559	Protected Theater - Add Unauthorized Ssh Key, Variant #1	ATT&CK:M1022,ATT&CK:M1042,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1098.004,CAMP.26.018,CVE-2022-20775,Control:Endpoint,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-560	Protected Theater - AMATERASTEALER, Fileless Payload Execution Via Powershell Httpclient, 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:UNC6758,CAMP.26.032,Control:Endpoint,Malware:AMATERASTEALER,NIST:CM-11,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-561	Protected Theater - ANYDESK, FLOXIF, Communicates With C2, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,CAMP.26.029,Control:Endpoint,Malware:ANYDESK,Malware:FLOXIF,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-562	Protected Theater - ANYDESK, FLOXIF, Drops Malicious Dll Symsrv.Dll, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,CAMP.26.029,Control:Endpoint,Malware:ANYDESK,Malware:FLOXIF,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-563	Protected Theater - APT42, TAMECAT, Contacts C2 Server, Variant #1	ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,Actor:APT42,CAMP.26.028,Control:Endpoint,Malware:TAMECAT,NIST:AC-4,NIST:CM-7,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-564	Protected Theater - APT42, TAMECAT, Powershell Execution, 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:APT42,CAMP.26.028,Control:Endpoint,Malware:TAMECAT,NIST:CM-11,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-565	Protected Theater - Clear Windows Vpn Event Log, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1029,ATT&CK:M1041,ATT&CK:T1070.001,CAMP.26.049,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-566	Protected Theater - Create Zip Archive Header Via Set Command, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1040,ATT&CK:M1049,ATT&CK:T1027,CAMP.26.039,CWE:173,CWE:20,CWE:697,CWE:74,Control:Endpoint,NIST:AC-4,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-567	Protected Theater - DINODANCE, WGET, Execute Obfuscated Command For Dns Resolution, Variant #1	ATT&CK:Defense Evasion,ATT&CK:T1027.010,Actor:UNC6740,CAMP.26.023,Control:Endpoint,Malware:DINODANCE,Malware:WGET,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-568	Protected Theater - Establish Reverse Shell, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,CAMP.26.034,Control:Endpoint,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-569	Protected Theater - Execute Arcgis Trojanized Installer, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,CAMP.26.050,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A108-570	Protected Theater - Execute Obfuscated Hta Payload Via Comspec, Variant #1	ATT&CK:Execution,ATT&CK:M1038,ATT&CK:T1059.003,CAMP.26.043,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-571	Protected Theater - Executes And Connects To C2 Domain, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,CAMP.26.029,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-572	Protected Theater - LIGHTPHOENIX, Copy To Staging Directory With, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:LIGHTPHOENIX,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-573	Protected Theater - LIGHTPHOENIX, Demonstrates C2 Communication, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,CAMP.26.029,Control:Endpoint,Malware:LIGHTPHOENIX,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-574	Protected Theater - LIGHTPHOENIX, Demonstrates File Drop, Variant #1	ATT&CK:Execution,ATT&CK:M1026,ATT&CK:M1038,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1049,ATT&CK:T1059.001,CAMP.26.029,Control:Endpoint,Malware:LIGHTPHOENIX,NIST:CM-11,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-575	Protected Theater - Permit Root Login Via Ssh, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.001,CAMP.26.018,CVE-2022-20775,CWE:284,Control:Endpoint,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-576	Protected Theater - Store Encoded Data In Registry, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1024,ATT&CK:Persistence,ATT&CK:T1112,CAMP.26.039,CWE:15,CWE:732,Control:Endpoint,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-577	Protected Theater - SUPREMO, Connects To C2, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,CAMP.26.049,Control:Endpoint,Malware:SUPREMO,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-578	Protected Theater - SUPREMO, Persistence Via Windows Service, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,CAMP.26.049,CWE:284,Control:Endpoint,Malware:SUPREMO,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-579	Protected Theater - TAMECAT, Execute Informations Module, Variant #1	ATT&CK:Discovery,ATT&CK:T1082,Actor:APT42,CAMP.26.028,Control:Endpoint,Malware:TAMECAT,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-580	Protected Theater - TURTLESHELL, Archive Browser Artifacts With Find And Cpio, Variant #1	ATT&CK:Credential Access,ATT&CK:M1027,ATT&CK:M1042,ATT&CK:M1051,ATT&CK:M1054,ATT&CK:T1555,Actor:UNC6721,CAMP.26.033,Control:Endpoint,Malware:TURTLESHELL,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-581	Protected Theater - TURTLESHELL, Archive User Documents With Find And Cpio, Variant #1	ATT&CK:Collection,ATT&CK:T1074.001,Actor:UNC6721,CAMP.26.033,Control:Endpoint,Malware:TURTLESHELL,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-582	Protected Theater - TURTLESHELL, Stage Sam Hive, Variant #1	ATT&CK:Credential Access,ATT&CK:M1017,ATT&CK:M1026,ATT&CK:M1027,ATT&CK:M1028,ATT&CK:T1003.002,Actor:UNC6721,CAMP.26.033,Control:Endpoint,Malware:TURTLESHELL,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-583	Protected Theater - UNC3313, ATERA, C2 Communication, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC3313,CAMP.26.029,Control:Endpoint,Malware:ATERA,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-584	Protected Theater - UNC3313, ATERA, Configures The Agent Service To Restart On Failure, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC3313,CAMP.26.029,CWE:284,Control:Endpoint,Malware:ATERA,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-585	Protected Theater - UNC3313, ATERA, Install Msi And Drop Agent.Exe, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC3313,CAMP.26.029,Control:Endpoint,Malware:ATERA,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-586	Protected Theater - UNC3313, ATERA, Msi Installation, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC3313,CAMP.26.029,Control:Endpoint,Malware:ATERA,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-587	Protected Theater - UNC3313, ATERA, Rmm Msi Execution, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC3313,CAMP.26.029,Control:Endpoint,Malware:ATERA,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-588	Protected Theater - UNC3313, PDQ, Executes Msi Installer, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC3313,CAMP.26.029,Control:Endpoint,Malware:PDQ,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-589	Protected Theater - UNC3313, SWANSOUL, Downloads A Payload, 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:UNC3313,CAMP.26.029,Control:Endpoint,Malware:SWANSOUL,NIST:CM-11,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-590	Protected Theater - UNC5667, Connects To C2, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A108-591	Protected Theater - UNC5667, Drops Payload `Powersh.Exe`, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-592	Protected Theater - UNC5667, Drops Photoacq.Log, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A108-593	Protected Theater - UNC5667, Executes File.Exe Dropping Srvspool.Exe, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1038,ATT&CK:M1045,ATT&CK:T1036.005,Actor:UNC5667,CAMP.26.029,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-594	Protected Theater - UNC5667, Executes File.Exe Leading To C2 Communication, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-595	Protected Theater - UNC5667, Executes Srvspool.Exe To Masquerade As Spooler Service, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1038,ATT&CK:M1045,ATT&CK:T1036.005,Actor:UNC5667,CAMP.26.029,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-596	Protected Theater - UNC5667, FRONTLOAD, Connects To C2, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:FRONTLOAD,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-597	Protected Theater - UNC5667, FRONTLOAD, Drops Secure System.Exe, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:FRONTLOAD,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-598	Protected Theater - UNC5667, GLOWSTICK, PROTONGLOW, SILVERLIME, Connects To C2, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:GLOWSTICK,Malware:PROTONGLOW,Malware:SILVERLIME,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-599	Protected Theater - UNC5667, GLOWSTICK, PROTONGLOW, SILVERLIME, Drops Miazaki.Dll, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:GLOWSTICK,Malware:PROTONGLOW,Malware:SILVERLIME,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-600	Protected Theater - UNC5667, GLOWSTICK, PROTONGLOW, SILVERLIME, Establishes Persistence Via Com Hijacking, Variant	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1546.015,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:GLOWSTICK,Malware:PROTONGLOW,Malware:SILVERLIME,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-601	Protected Theater - UNC5667, GREYBAG, C2 Communication, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:GREYBAG,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-602	Protected Theater - UNC5667, GREYMIRROR, HORSESHOE, For Persistence Via Registry Run Key, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:GREYMIRROR,Malware:HORSESHOE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-603	Protected Theater - UNC5667, GREYMIRROR, HORSESHOE, POTATOWALL, Via File Copy And Registry Run Key, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:GREYMIRROR,Malware:HORSESHOE,Malware:POTATOWALL,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-604	Protected Theater - UNC5667, GREYMIRROR, PROTONGLOW, Connects To A C2 Server, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:GREYMIRROR,Malware:PROTONGLOW,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-605	Protected Theater - UNC5667, GREYMIRROR, PROTONGLOW, Creates A Service For Persistence, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC5667,CAMP.26.029,CWE:284,Control:Endpoint,Malware:GREYMIRROR,Malware:PROTONGLOW,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-606	Protected Theater - UNC5667, GREYMIRROR, PROTONGLOW, Drops Sysprocupdate.Exe, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:GREYMIRROR,Malware:PROTONGLOW,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-607	Protected Theater - UNC5667, GREYMIRROR, PROTONGLOW, Drops The Executable, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:GREYMIRROR,Malware:PROTONGLOW,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A108-608	Protected Theater - UNC5667, GREYMIRROR, PROTONGLOW, Executes And Connects To C2, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:GREYMIRROR,Malware:PROTONGLOW,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-609	Protected Theater - UNC5667, GREYMIRROR, PROTONGLOW, To Persist Via Service Creation, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC5667,CAMP.26.029,CWE:284,Control:Endpoint,Malware:GREYMIRROR,Malware:PROTONGLOW,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-610	Protected Theater - UNC5667, HORSESHOE, Backdoor Persistence Staging, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1038,ATT&CK:M1045,ATT&CK:T1036.005,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:HORSESHOE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-611	Protected Theater - UNC5667, HORSESHOE, Create Persistence Service, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC5667,CAMP.26.029,CWE:284,Control:Endpoint,Malware:HORSESHOE,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-612	Protected Theater - UNC5667, HORSESHOE, Move Executable To Appdata, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1038,ATT&CK:M1045,ATT&CK:T1036.005,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:HORSESHOE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-613	Protected Theater - UNC5667, HORSESHOE, Registry Run Key, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:HORSESHOE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-614	Protected Theater - UNC5667, Initiates C2 Communication, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-615	Protected Theater - UNC5667, IVYPHOENIX, Contacts C2 Domain Cipheredge.Pro, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:IVYPHOENIX,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-616	Protected Theater - UNC5667, IVYPHOENIX, Persistence Via Masquerading Windows Service, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC5667,CAMP.26.029,CWE:284,Control:Endpoint,Malware:IVYPHOENIX,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-617	Protected Theater - UNC5667, LIGHTPHOENIX, Beacons To A C2 Server, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:LIGHTPHOENIX,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-618	Protected Theater - UNC5667, LIGHTPHOENIX, Connects To C2, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:LIGHTPHOENIX,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-619	Protected Theater - UNC5667, LIGHTPHOENIX, Creates A Scheduled Task For, 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:UNC5667,CAMP.26.029,Control:Endpoint,Malware:LIGHTPHOENIX,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-620	Protected Theater - UNC5667, LIGHTPHOENIX, Persistence Via Scheduled Task, 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:UNC5667,CAMP.26.029,Control:Endpoint,Malware:LIGHTPHOENIX,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-621	Protected Theater - UNC5667, LIGHTPHOENIX, Second Stage C2 Beacon, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:LIGHTPHOENIX,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-622	Protected Theater - UNC5667, POTATOWALL, Persistence Via Scheduled Task, 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:UNC5667,CAMP.26.029,Control:Endpoint,Malware:POTATOWALL,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-623	Protected Theater - UNC5667, POTATOWALL, Persistence Via Scheduled Task, Variant #2	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:UNC5667,CAMP.26.029,Control:Endpoint,Malware:POTATOWALL,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-624	Protected Theater - UNC5667, POTATOWALL, Persistence Via Windows Service, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC5667,CAMP.26.029,CWE:284,Control:Endpoint,Malware:POTATOWALL,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-625	Protected Theater - UNC5667, POTATOWALL, Scheduled Task 'Nova Service', 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:UNC5667,CAMP.26.029,Control:Endpoint,Malware:POTATOWALL,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-627	Protected Theater - UNC5667, PROTONGLOW, Drops Second Stage Payload, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:PROTONGLOW,OS:Windows:10,OS:Windows:11,RunAs:Admin,Src:Internal:Trusted
A108-628	Protected Theater - UNC5667, PROTONGLOW, Execute To Beacon To C2, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:PROTONGLOW,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-629	Protected Theater - UNC5667, PROTONGLOW, Execute To Drop Payload, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:PROTONGLOW,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-630	Protected Theater - UNC5667, PROTONGLOW, Scheduled Task 'Googleupdater', 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:UNC5667,CAMP.26.029,Control:Endpoint,Malware:PROTONGLOW,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-631	Protected Theater - UNC5667, PROTONGLOW, SILVERLIME, Drops Mononoke.Exe, Variant #1	ATT&CK:Execution,ATT&CK:M1038,ATT&CK:T1059.003,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:PROTONGLOW,Malware:SILVERLIME,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-632	Protected Theater - UNC5667, PROTONGLOW, Via Scheduled Task (Sysprocupdate.Exe), 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:UNC5667,CAMP.26.029,Control:Endpoint,Malware:PROTONGLOW,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-633	Protected Theater - UNC5667, ROADSIGN, C2 Beacon, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:ROADSIGN,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-634	Protected Theater - UNC5667, ROADSIGN, Executes Batch Script Masquerading As An Ini File, Variant #1	ATT&CK:Execution,ATT&CK:M1038,ATT&CK:T1059.003,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:ROADSIGN,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-635	Protected Theater - UNC5667, RUBBERAXE, C2 Beacon, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:RUBBERAXE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-636	Protected Theater - UNC5667, RUBBERAXE, Creates Scheduled Task, 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:UNC5667,CAMP.26.029,Control:Endpoint,Malware:RUBBERAXE,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-637	Protected Theater - UNC5667, RUBBERAXE, Dropper Connecting To C2, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:RUBBERAXE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A108-638	Protected Theater - UNC5667, RUBBERAXE, Drops The Payload, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:RUBBERAXE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A108-639	Protected Theater - UNC5667, RUBBERAXE, Execute Attachment.Xls To Drop Payload, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,CAMP.26.029,Control:Endpoint,Malware:RUBBERAXE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A108-641	Protected Theater - UNC5667, RUBBERAXE, For Persistence, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC5667,CAMP.26.029,CWE:284,Control:Endpoint,Malware:RUBBERAXE,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-642	Protected Theater - UNC5667, RUBBERAXE, Persistence Via Scheduled Task (Pic.Log), 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:UNC5667,CAMP.26.029,Control:Endpoint,Malware:RUBBERAXE,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-643	Protected Theater - UNC5669, REALBREEZE, To Drop The Secondary Executable Payload, Variant #1	ATT&CK:Defense Evasion,ATT&CK:T1140,Actor:UNC5669,CAMP.26.049,Control:Endpoint,Malware:REALBREEZE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-644	Protected Theater - UNC5669, REMCOS, C2 Beaconing, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1050,ATT&CK:T1218.011,Actor:UNC5669,CAMP.26.049,CWE:114,Control:Endpoint,Malware:REMCOS,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
A108-645	Protected Theater - UNC5669, REMCOS, Executes To Connect To C2, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1038,ATT&CK:M1044,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1574.001,CWE:114,CWE:427,Control:Endpoint,Malware:REMCOS,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-646	Protected Theater - UNC5669, XWORM, Communicates With C2, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5669,CAMP.26.049,Control:Endpoint,Malware:XWORM,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-647	Protected Theater - UNC5669, XWORM, Drops A Plugin Dll, Variant #1	ATT&CK:Execution,ATT&CK:M1038,ATT&CK:T1129,Actor:UNC5669,CAMP.26.049,CWE:114,Control:Endpoint,Malware:XWORM,NIST:CM-11,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-648	Protected Theater - UNC5669, XWORM, Establishes Persistence Via A Registry Run Key, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC5669,CAMP.26.049,Control:Endpoint,Malware:XWORM,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-649	Protected Theater - UNC5669, XWORM, To Establish C2 Communication, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5669,CAMP.26.049,Control:Endpoint,Malware:XWORM,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-650	Protected Theater - UNC6674, Creates A Run Key For Persistence, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC6674,CAMP.26.015,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-651	Protected Theater - UNC6674, PURERAT, Connects To Command And Control, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6674,CAMP.26.015,Control:Endpoint,Malware:PURERAT,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-652	Protected Theater - UNC6674, PURERAT, Drops Secondary Executable, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6674,CAMP.26.015,Control:Endpoint,Malware:PURERAT,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-653	Protected Theater - UNC6674, PURERAT, For Persistence Via Scheduled Task, 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:UNC6674,CAMP.26.015,Control:Endpoint,Malware:PURERAT,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-654	Protected Theater - UNC6674, Sets Hidden And System Attributes On A Directory, Variant #1	ATT&CK:Defense Evasion,ATT&CK:T1564.001,Actor:UNC6674,CAMP.26.015,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-655	Protected Theater - UNC6674, VALLEYRAT, Hides Directory Using Attrib, Variant #1	ATT&CK:Defense Evasion,ATT&CK:T1564.001,Actor:UNC6674,CAMP.26.015,Control:Endpoint,Malware:VALLEYRAT,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-656	Protected Theater - UNC6674, VALLEYRAT, Via Registry Run Key, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC6674,CAMP.26.015,Control:Endpoint,Malware:VALLEYRAT,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-657	Protected Theater - UNC6676, Creates A Hidden .Vscode Directory For Staging, Variant #1	ATT&CK:Defense Evasion,ATT&CK:T1564.001,Actor:UNC6676,CAMP.26.041,Control:Endpoint,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-658	Protected Theater - UNC6723, Connects To C2 Domain, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6723,CAMP.26.051,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-659	Protected Theater - UNC6723, Drops Rclone Utility, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6723,CAMP.26.051,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-660	Protected Theater - UNC6723, Javascript Downloader Contacts C2, Variant #1	ATT&CK:Execution,ATT&CK:M1021,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:M1042,ATT&CK:T1059.007,Actor:UNC6723,CAMP.26.051,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-661	Protected Theater - UNC6753, SPARKRAT, C2 Communication Via Ip, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6753,CAMP.26.047,Control:Endpoint,GLOBAL.26.004,Malware:SPARKRAT,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-662	Protected Theater - UNC6780, SANDCLOCK, C2 Communication, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6780,CAMP.26.036,Control:Endpoint,Malware:SANDCLOCK,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-663	Protected Theater - UNC6780, SANDCLOCK, Executes Dropper To Stage Script, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6780,CAMP.26.036,Control:Endpoint,Malware:SANDCLOCK,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-664	Protected Theater - UNC6780, SANDCLOCK.SH, C2 Exfiltration, Variant #1	ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,Actor:UNC6780,CAMP.26.036,Control:Endpoint,Malware:SANDCLOCK.SH,NIST:AC-4,NIST:CM-7,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-665	Protected Theater - UNC6780, SANDCLOCK.SH, Data Aggregation, Variant #1	ATT&CK:Collection,ATT&CK:T1074.001,Actor:UNC6780,CAMP.26.036,Control:Endpoint,Malware:SANDCLOCK.SH,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-666	Protected Theater - UNC6781, Executes A Base64 Encoded Powershell Command To Download A Payload, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1040,ATT&CK:M1049,ATT&CK:T1027,Actor:UNC6781,CAMP.26.050,CWE:173,CWE:20,CWE:697,CWE:74,Control:Endpoint,NIST:AC-4,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-667	Protected Theater - UNC6781, Executes A Malicious Installer Triggering A C2 Connection, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6781,CAMP.26.050,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-668	Protected Theater - UNC6781, Executes Nsis Installer To Download Second Stage, Variant #1	ATT&CK:Execution,ATT&CK:M1033,ATT&CK:M1038,ATT&CK:M1047,ATT&CK:M1049,ATT&CK:T1059.006,Actor:UNC6781,CAMP.26.050,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-669	Protected Theater - WAVESHAPER.V2, Persistence Via Registry Run Key, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,CAMP.26.042,Control:Endpoint,Malware:WAVESHAPER.V2,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-670	Protected Theater - WINDSTRIKE, Add Defender Exclusion Via Powershell, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.001,Actor:UNC6715,CAMP.26.020,CWE:284,Control:Endpoint,Malware:WINDSTRIKE,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-671	Protected Theater - XWORM, Persistence Via Startup Folder Shortcut, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,CAMP.26.049,Control:Endpoint,Malware:XWORM,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted

New Files

A total of 111 new files have been added to the File Library with this update. This includes 111 malicious files.

Malicious Files

File MD5	Tags
027346a7bf701a3c25bc2493d86c9181	Malware_Type:LAUNCHER,Group:Validation,Malware:SHADOWRICE
03d1be17f27fdfe955a1c6bcd1835116	Malware:TAMECAT,Group:Validation
047ecfaf35b24ec74b523df17a745365	Malware:VALLEYRAT,Malware_Type:BACKDOOR,Group:Validation
04e3073b3cd5c5bfcde6f575ecf6e8c1	Malware_Type:BACKDOOR,Malware:WAVESHAPER.V2.PS,Group:Validation
089e2872016f75a5223b5e02c184dfec	Malware_Type:DOWNLOADER,Group:Validation
0a60635b2aec352d7b5162701ec612a8	Group:Validation
0e7fcb91d104df699e159272d17ed654	Group:Validation
0fad9f97489c8a175e7c66c3dba59a97	Malware:SPARKRAT,Malware_Type:BACKDOOR,Group:Validation
161746b1ca0e6c9a7c94900328422271	Malware:POTATOWALL,Malware_Type:BACKDOOR,Group:Validation
16644838d9d953d8f185edb811aba817	Group:Validation
1929da3ef904efb8c940679045452321	Group:Validation
1a86ed697e24731b88e5e591c6ecfb91	Group:Validation,Malware:PROTONGLOW,Malware_Type:BACKDOOR
1e1c83b9680029ad4a9f8d3b3ac93197	Group:Validation
20cf4b12fa866c28fe7523a717340e0d	Group:Validation
23366ac08fa76f237ba90b3373e6cf91	Group:Validation
25c632cd2f529ba142fa706205ac00c9	Group:Validation
26b99e20c5cf5360d5875f280eb6c091	Group:Validation,Malware_Type:BACKDOOR,Malware:REMCOS

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
29dee8b421fab8eb1e67c7451aa227f8	Malware_Type:BACKDOOR,Malware:PURERAT,Group:Validation
2f982d975c46fca1ae455469db6c221d	Malware:WAVESHAPER.V2.MACHO,Malware_Type:BACKDOOR,Group:Validation
376884baaa4b9505792afc81cdedda42	Group:Validation
39633967c5dfdaeea577cbaeb9837374	Group:Validation,Malware:SHADOWRICE
3ed14e7b4ef3602093fd27226d856de1	Group:Validation
439c0a0a46627bd166e08436f383ad56	Malware:STAGEHAND,Malware_Type:DOWNLOADER,Group:Validation
45146b7913dac0de49c391733d38e5c8	Group:Validation,Malware_Type:BACKDOOR,Malware:XWORM
47198c5e434f94fa58f07553b398b46e	Group:Validation,Malware:ATERA
477293f80461713d51a98a24023d45e8	Group:Validation,Malware:ATERA
484730d6e8a5e03f3d795062e1c5b199	Group:Validation,Malware:SCREENCONNECT
487297b619c276522d1b189a362540c1	Group:Validation
497c1ad79c4ef5425eb8a7e4f49efc8b	Group:Validation
4b7731b802165f8d6b79c21c789bb366	Group:Validation
4fb2c43e530ac14e42d17598a5b5550d	Group:Validation,Malware_Type:BACKDOOR,Malware:XWORM
591aae15106147bdb5bc7b26049b943f	Group:Validation
5965ca0388612b0ddff14d59c22936bb	Malware:TAMECAT,Group:Validation
5ad8606a76ab669c4a140fc2eddb7e06	Group:Validation
5e596fc390a0205d202dda141aed2ef1	Group:Validation
694a1947b2eb5cf7f4aad483fcccbf67	Malware:BEAVERTAIL,Group:Validation
6b85c4279a9944cd5f50aa62af5a380a	Malware:WAVESHAPER.V2.MACHO,Malware_Type:BACKDOOR,Group:Validation
6d1d4e938ed1e46210375308ef3bcb08	Malware_Type:LAUNCHER,Group:Validation,Malware:DINODANCE
7236f1a51da141e422d553e36ef6c9d0	Malware_Type:LAUNCHER,Group:Validation,Malware:DINODANCE
723daa5daf48484aaaf708d7e058742f	Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
7574cf2c64f35161ab1292e2f532aabf	Group:Validation,Malware_Type:DOWNLOADER
7658962ae060a222c0058cd4e979bfa1	Malware:SILKBELL,Malware_Type:DOWNLOADER,Group:Validation
79b075dc4fce7321f3be049719f3ce27	Group:Validation,Malware:REMCOM
79e0beb2756eef59a25174dfd6c8f71c	Malware:BEAVERTAIL,Group:Validation
7a722d67f0516572b2315b2244b43552	Group:Validation,Malware_Type:UTILITY
7a9ddef00f69477b96252ca234fcbeeb	Malware_Type:BACKDOOR,Malware:WAVESHAPER.V2.MACHO,Group:Validation
7c21371e257042d7618b7b8218591a0e	Group:Validation,Malware:REALBREEZE
7e13d678028e93739d11a0ea6a8fce87	Group:Validation,Malware_Type:DROPPER
7e3c10bb262865a0daaf5c88a2fe7a79	Group:Validation
7e6df98beeba4755a7c3e992f849ebc7	Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
805c08686e755c063a0bb460bdf9dcc4	Group:Validation,Malware:SANDCLOCK
82de35e133dd4936f3a8b2a69b30c9a4	Group:Validation
837f867ad708295129969c13cfc22992	Group:Validation
8bddcad83361397840fdb1ee97d8a6a6	Group:Validation,Malware:SANDCLOCK
8ca60ad84b6f6b3b9352e77cd8682d81	Malware:SANDCLOCK,Group:Validation
8cf49650b7a000d09e8af77c314dfdad	Malware:QUICKSTEP,Group:Validation
90e8e227ba8bef0ea7e0212b5b1e0d4c	Malware_Type:BACKDOOR,Malware:WAVESHAPER.V2.PS,Group:Validation
91583b45e2d63ab7eab4c9d2a7a113a4	Group:Validation
9663665850cdd8fe12e30a671e5c4e6f	Malware_Type:BACKDOOR,Malware:WAVESHAPER.V2.PY,Group:Validation
98294a2c838eaf63fe94cccf52af3ce8	Malware:PANICPOACH,Malware_Type:DATA_MINER,Group:Validation
998fea0bac8471af3058b9f17d147b45	Malware_Type:BACKDOOR,Malware:WAVESHAPER.V2.MACHO,Group:Validation
999e4781d1772bfd711ce9441cfada84	Group:Validation
9c6c67344fecd8ff8dbbee877aad7efc	Malware:PANICPOACH,Malware_Type:DATA_MINER,Group:Validation
a114fd44b8399c5a9e246de89b397076	Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
a2d88379190901d13a925b0253bba2df	Group:Validation
a35a0ccb200134d136a00f78eb015c40	Malware:WAVESHAPER.V2.MACHO,Malware_Type:BACKDOOR,Group:Validation
aaf072a034f20c58af830a12998317eb	Malware:BEAVERTAIL,Group:Validation
ab8bab19130296731d3d1d1afd628f1b	Malware:SOFTMETAL,Group:Validation
ac63f5537c290ea76ebb86b2eb24a4a9	Group:Validation,Malware_Type:DROPPER
ae60726d04bc06d0c623e567e8e9b241	Malware:SANDCLOCK,Group:Validation
b27922ddc9c75753bf503c407b01b4fa	Group:Validation
b43b51d2d3f864e76988e4e2ac10eb81	Malware_Type:DOWNLOADER,Group:Validation,Malware:TIREPATCH
b731bd186af22ad6022f155f55103eec	Malware_Type:BACKDOOR,Malware:WAVESHAPER.V2.MACHO,Group:Validation
b857ecc4f6b739dff7b93321e7788cab	Group:Validation
bdfe5efd0f34e023e91d4b3897635873	Group:Validation,Malware:REALBREEZE,Malware_Type:UTILITY
bed77abc7e12230439c0b53dd68ffaf7	Group:Validation,Malware_Type:DROPPER_MEMORY_ONLY,Malware:HORSESHOE
bfb4aa740748e60caf01f45bc81a3b2c	Group:Validation
c5169404fb9af53e87992f3d2b8c36e2	Group:Validation
c5b54a82ee798c3858a0fbac12ac742e	Group:Validation
c5f07af0e93bde3c3fc63b83cbaad112	Malware:WAVESHAPER.V2.PY,Malware_Type:BACKDOOR,Group:Validation
c72a28f660132ea571ac1bc7984d7267	Group:Validation
c73c308a137ff7805577042cc9e923e1	Group:Validation
c851e849c8442727eac69225203ee7f7	Group:Validation
c8f269d59279d3ba35284da2f8e6cbfc	Malware:TAMECAT,Group:Validation
cbf38082fcc1a92a366d2e43f68bfd84	Malware_Type:DROPPER_MEMORY_ONLY,Malware:AMATERASTEALER,Group:Validation
cc6b7d9e2fd7202d55e8c06012f256a8	Group:Validation
ccccd50bf5226af5b462e49d9a4a6912	Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
cfe841e08e589d53e5b520594085d457	Group:Validation,Malware:WAVESHAPER.V2.PS,Malware_Type:BACKDOOR
cffe67da05e2c61f7653d360c652995b	Malware_Type:BACKDOOR,Malware:WAVESHAPER.V2.PS,Group:Validation
d276b8c1660f264d64eff3474718509b	Group:Validation
d3527e6a049575471f90d20fd02613be	Group:Validation
d761a6a7ae9f2254bd81ac234033a8b8	Group:Validation,Malware:SANDCLOCK.SH
d7a0d2cb0191abc3f636f187def913bc	Malware_Type:DOWNLOADER,Group:Validation
d8fe440e7c86f6d319a0814de4b036d4	Group:Validation
d9a0ac3dc5f1302c4d722562ceefe9ed	Group:Validation
db7f4c82c732e8b107492cae419740ab	Malware_Type:DOWNLOADER,Malware:SILKBELL,Group:Validation
dbf02905b01f90ad6aded9bda22ce67a	Group:Validation
dc2978e7565292b7e52ec2701d3c7047	Malware:TAMECAT,Group:Validation
df50a51d4718bf0c7e7431e4db531961	Group:Validation
e00d80b341018c6bb6e06063f77e29d9	Group:Validation
e68d7ead1c2f5970541346ac8cb6f4fb	Group:Validation
e930b05efe23891d19bc354a4209be3e	Malware:MIMIKATZ,Group:Validation
eab01b2f0e030597be04fe0e1819face	Group:Validation,Malware_Type:LAUNCHER
eaffc2d2d00de417bb657a789938789d	Malware:WAVESHAPER.V2.MACHO,Malware_Type:BACKDOOR,Group:Validation
eb7635f4836c9e0aa4c315b18b051cb5	Malware_Type:DOWNLOADER,Malware:WAVESHAPER,Group:Validation
eccb72c35d9679ddddc1ace212d59200	Group:Validation
f256a9c7e68a249fe760019d19c022ce	Group:Validation
f93be01556d2f1c0994889540eddf3fb	Group:Validation,Malware:POTATOWALL,Malware_Type:BACKDOOR
fa4cee65cc0650d465b2bd0ef8a77c14	Malware_Type:LAUNCHER,Group:Validation,Malware:SHADOWRICE
fda501d63f3d2d74e05a63e0d51ee0cf	Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
fff08b0d0954c836157b6dca56b5513c	Group:Validation,Malware_Type:BACKDOOR,Malware:XWORM

Retired Security Content

With this release, 4 Actions have been retired.

Actions

VID	Name	Reason for Removal
A107-507	Command and Control - UNC1549, TWOSTROKE, Check-In, Variant #1	Content no longer meets Validation's standards of use
A107-520	Command and Control - UNC5667, GREYSHOT, Check-In, Variant #1	Content no longer meets Validation's standards of use
A107-521	Command and Control - UNC5667, IVYPHOENIX, Check-In, Variant #1	Content no longer meets Validation's standards of use
A107-534	Command and Control - UNC5667, SILVERLIME, Communication, Variant #1	Content no longer meets Validation's standards of use

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.