Mandiant

VHR20260306 - MARCH 6, 2026

The Mandiant Intelligence Validation Research Team (VRT) has published VHR20260306 - 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

- 382 Actions added
- 231 Files added

Release Highlights

- New Actions covering **UNC3313** (https://advantage.mandiant.com/actors/UNC3313), an Iran-nexus cyber espionage group observed targeting Middle Eastern government, telecommunications, and technology entities.
- New Actions covering **UNC1549** (https://advantage.mandiant.com/actors/UNC1549), a suspected Iranian cyber espionage cluster targeting energy, government, and defense sectors primarily in Saudi Arabia and the United Arab Emirates.
- New Actions covering **APT42** (https://advantage.mandiant.com/actors/APT42), an Iranian state-sponsored cyber espionage group tasked with conducting information collection and surveillance operations against individuals and organizations of strategic interest to the Iranian Government.
- New Actions covering **UNC5866** (https://advantage.mandiant.com/actors/UNC5866), a suspected Iran-nexus threat actor performing hacktivism and malware delivery campaigns.
- New Actions covering **UNC5667** (https://advantage.mandiant.com/actors/UNC5667), a suspected subcluster of the Iranian espionage actor UNC3313 primarily conducting custom malware deployment operations via spearphishing.
- New Actions covering **UNC6085** (https://advantage.mandiant.com/actors/UNC6085), a suspected Iranian cluster conducting surveillance and monitoring operations against the Iranian diaspora, activists, journalists, and the education sector, and leveraging the Telegram-based **HEAVYGRAM** (https://advantage.mandiant.com/malware/HEAVYGRAM) backdoor.

New Actions

A total of 382 Actions have been added to the content baseline with this update. This includes 295 Network Actions, 11 Host CLI Actions, and 76 Protected Theater Actions. All Actions in this release are tagged using the MITRE ATT&CK v17.1 framework.

Network Actions

VID	Name	Tags
A107-506	Command and Control - UNC1549, Task Request, Variant #1	ATT&CK:Command and Control,ATT&CK:Discovery,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1082,ATT&CK:T1083,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-507	Command and Control - UNC1549, TWOSTROKE, Check-In, 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,Actor:UNC1549,CWE:173,CWE:20,CWE:697,CWE:74,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:TWOSTROKE,NIST:AC-4,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-508	Command and Control - UNC1549, TWOSTROKE, Communication, 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,Actor:UNC1549,CWE:173,CWE:20,CWE:697,CWE:74,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:AC-4,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-509	Command and Control - UNC1549, TWOSTROKE, Exfiltration, Variant #2	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-510	Command and Control - UNC3313, ATERA, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-511	Command and Control - UNC3313, ATERA, Command Request, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-512	Command and Control - UNC3313, ATERA, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-513	Command and Control - UNC3313, OPENGAZE, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:OPENGAZE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-514	Command and Control - UNC3313, OPENGAZE, Command Request, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:OPENGAZE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-515	Command and Control - UNC3313, SYNCRO, Check-In, 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:T1082,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SYNCRO,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-516	Command and Control - UNC3313, SYNCRO, Check-In, Variant #2	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102.002,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:SYNCRO,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-517	Command and Control - UNC3313, SYNCRO, Communication, Variant #1	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,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SYNCRO,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-518	Command and Control - UNC3313, SYNCRO, Communication, Variant #2	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,CWE:284,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SYNCRO,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-519	Command and Control - UNC5667, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573.002,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-520	Command and Control - UNC5667, GREYSHOT, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573.002,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYSHOT,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-521	Command and Control - UNC5667, IVYPHOENIX, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:IVYPHOENIX,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-522	Command and Control - UNC5667, LIGHTPHOENIX, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573,Actor:UNC5667,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
A107-523	Command and Control - UNC5667, LIGHTPHOENIX, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTPHOENIX,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-524	Command and Control - UNC5667, LIGHTPHOENIX, Communication, Variant #2	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,Actor:UNC5667,Control:DLP,Control:NGFW,Control:Proxy,Control:WAF,Malware:LIGHTPHOENIX,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-525	Command and Control - UNC5667, LIGHTPHOENIX, External IP Discovery, Variant #1	ATT&CK:Command and Control,ATT&CK:Discovery,ATT&CK:M1031,ATT&CK:T1016.001,ATT&CK:T1071.001,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTPHOENIX,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-526	Command and Control - UNC5667, LIGHTPHOENIX, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,ATT&CK:T1132.001,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTPHOENIX,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-527	Command and Control - UNC5667, LIGHTPHOENIX, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1132.001,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTPHOENIX,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-528	Command and Control - UNC5667, POTATOWALL, Telegram, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POTATOWALL,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-529	Command and Control - UNC5667, POTATOWALL, Telegram, Variant #2	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POTATOWALL,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-530	Command and Control - UNC5667, POTATOWALL, Telegram, Variant #3	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POTATOWALL,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-531	Command and Control - UNC5667, POTATOWALL, Telegram, Variant #4	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POTATOWALL,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-532	Command and Control - UNC5667, RUBBERAXE, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:RUBBERAXE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-533	Command and Control - UNC5667, RUBBERAXE, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:RUBBERAXE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-534	Command and Control - UNC5667, SILVERLIME, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,ATT&CK:T1573.002,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SILVERLIME,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-535	Command and Control - UNC5667, SOFTMETAL, Malware Download List, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SOFTMETAL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-536	Command and Control - UNC5667, STAGEHAND, Check-in, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:STAGEHAND,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-537	Command and Control - UNC5667, STAGEHAND, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:Discovery,ATT&CK:M1031,ATT&CK:T1033,ATT&CK:T1071.001,ATT&CK:T1082,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:STAGEHAND,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-538	Command and Control - UNC5866, SACREDGAME, C2, Variant #1	ATT&CK:Command and Control,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573,Actor:UNC5866,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SACREDGAME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-539	Command and Control - UNC6085, BADMOVIE, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADMOVIE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-540	Command and Control - UNC6085, BADMOVIE, Status Update, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADMOVIE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-541	Command and Control - UNC6085, BADMOVIE, Status Update, Variant #2	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADMOVIE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-542	Command and Control - UNC6085, BADMOVIE, Telegram, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADMOVIE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-543	Command and Control - UNC6085, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1071.001,ATT&CK:T1567,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-544	Command and Control - UNC6085, HEAVYGRAM, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HEAVYGRAM,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-545	Command and Control - UNC6085, LIGHTMASS, C2 Configuration Retrieval from GitHub Gist, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTMASS,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-546	Command and Control - UNC6085, LIGHTMASS, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTMASS,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-547	Command and Control - UNC6085, LIGHTMASS, Command Polling, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTMASS,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-548	Command and Control - UNC6085, Telegram Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-549	Command and Control - UNC6085, Telegram Check-In, Variant #2	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-550	Command and Control - UNC6085, Telegram Command Polling, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-551	Command and Control - UNC6085, Telegram Command Polling, Variant #2	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-552	Command and Control - UNC6085, Telegram Status Update, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-553	Command and Control - UNC6085, Telegram, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-565	Malicious File Transfer - APT42, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-566	Malicious File Transfer - APT42, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,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
A107-567	Command and Control - APT42, POWERPUG, Telegram Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:APT42,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POWERPUG,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-568	Malicious File Transfer - APT42, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-569	Malicious File Transfer - APT42, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-570	Malicious File Transfer - APT42, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-571	Malicious File Transfer - APT42, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-572	Malicious File Transfer - APT42, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-573	Malicious File Transfer - APT42, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-574	Malicious File Transfer - APT42, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-575	Malicious File Transfer - APT42, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-576	Malicious File Transfer - APT42, POWERPUG, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POWERPUG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-577	Malicious File Transfer - APT42, POWERPUG, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POWERPUG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-578	Malicious File Transfer - APT42, POWERPUG, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POWERPUG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-579	Malicious File Transfer - APT42, SOSHISMITH, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SOSHISMITH,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-580	Malicious File Transfer - APT42, SOSHISMITH, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SOSHISMITH,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-581	Malicious File Transfer - DCPHOENIX, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DCPHOENIX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-582	Malicious File Transfer - DCPHOENIX, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DCPHOENIX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-583	Malicious File Transfer - LIGHTPHOENIX, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTPHOENIX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-584	Malicious File Transfer - LIGHTPHOENIX, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTPHOENIX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-585	Malicious File Transfer - NETSCAN, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NETSCAN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-586	Malicious File Transfer - NETSCAN, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NETSCAN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-587	Malicious File Transfer - UNC1549, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-588	Command and Control - APT42, Telegram Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,ATT&CK:T1567.002,Actor:APT42,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-589	Malicious File Transfer - UNC1549, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-590	Malicious File Transfer - UNC1549, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-591	Malicious File Transfer - UNC1549, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-592	Malicious File Transfer - UNC1549, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-593	Malicious File Transfer - UNC1549, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-594	Malicious File Transfer - UNC1549, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-595	Malicious File Transfer - UNC1549, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,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
A107-596	Malicious File Transfer - UNC1549, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-597	Malicious File Transfer - UNC1549, LIGHTRAIL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTRAIL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-598	Malicious File Transfer - UNC1549, MINIBIKE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MINIBIKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-599	Malicious File Transfer - UNC1549, POLLBLEND, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POLLBLEND,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-600	Malicious File Transfer - UNC1549, POLLBLEND, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POLLBLEND,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-601	Malicious File Transfer - UNC1549, POLLREGISTER, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POLLREGISTER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-602	Malicious File Transfer - UNC1549, POLLREGISTER, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POLLREGISTER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-603	Malicious File Transfer - UNC1549, POLLREGISTER, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POLLREGISTER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-604	Malicious File Transfer - UNC1549, POLLREGISTER, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POLLREGISTER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-605	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-606	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-607	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-608	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-609	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-610	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #15	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-611	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #16	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-612	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #17	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-613	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #18	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-614	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #19	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-615	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #20	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-616	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #21	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-617	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #22	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-618	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #23	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-619	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #24	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-620	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #25	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-621	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #26	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-622	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #27	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-623	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #28	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-624	Command and Control - UNC1549, POLARDROP, Exfiltration, Variant #1	ATT&CK:Collection,ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1005,ATT&CK:T1041,ATT&CK:T1071.001,Actor:UNC1549,CWE:200,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POLARDROP,NIST:AC-23,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-625	Command and Control - UNC1549, POLARDROP, Check-In, Variant #2	ATT&CK:Command and Control,ATT&CK:Discovery,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1082,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POLARDROP,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-626	Command and Control - UNC1549, POLARDROP, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POLARDROP,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-627	Command and Control - UNC1549, LIGHTRAIL, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:LIGHTRAIL,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-628	Command and Control - UNC1549, CREDSTROKE, Exfiltration, Variant #2	ATT&CK:Command and Control,ATT&CK:Credential Access,ATT&CK:Exfiltration,ATT&CK:M1027,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,ATT&CK:T1555.003,Actor:UNC1549,CWE:522,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CREDSTROKE,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-629	Command and Control - UNC1549, CREDSTROKE, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CREDSTROKE,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-630	Command and Control - UNC1549, CREDSTROKE, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CREDSTROKE,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-631	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-632	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-633	Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-634	Malicious File Transfer - UNC3313, ATERA, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-635	Malicious File Transfer - UNC3313, ATERA, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-636	Malicious File Transfer - UNC3313, ATERA, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-637	Malicious File Transfer - UNC3313, ATERA, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-638	Malicious File Transfer - UNC3313, ATERA, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-639	Malicious File Transfer - UNC3313, ATERA, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-640	Malicious File Transfer - UNC3313, ATERA, Download, Variant #15	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-641	Malicious File Transfer - UNC3313, ATERA, Download, Variant #16	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-642	Malicious File Transfer - UNC3313, ATERA, Download, Variant #17	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-643	Malicious File Transfer - UNC3313, ATERA, Download, Variant #18	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-644	Malicious File Transfer - UNC3313, ATERA, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-645	Malicious File Transfer - UNC3313, ATERA, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-646	Malicious File Transfer - UNC3313, ATERA, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-647	Malicious File Transfer - UNC3313, ATERA, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-648	Malicious File Transfer - UNC3313, ATERA, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-649	Malicious File Transfer - UNC3313, ATERA, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-650	Malicious File Transfer - UNC3313, ATERA, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-651	Malicious File Transfer - UNC3313, ATERA, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-652	Malicious File Transfer - UNC3313, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-653	Malicious File Transfer - UNC3313, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,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
A107-654	Malicious File Transfer - UNC3313, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-655	Malicious File Transfer - UNC3313, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-656	Malicious File Transfer - UNC3313, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-657	Malicious File Transfer - UNC3313, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-658	Malicious File Transfer - UNC3313, Download, Variant #15	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-659	Malicious File Transfer - UNC3313, Download, Variant #16	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-660	Malicious File Transfer - UNC3313, Download, Variant #17	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-661	Malicious File Transfer - UNC3313, Download, Variant #18	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-662	Malicious File Transfer - UNC3313, Download, Variant #19	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-663	Malicious File Transfer - UNC3313, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,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
A107-664	Malicious File Transfer - UNC3313, Download, Variant #20	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-665	Malicious File Transfer - UNC3313, Download, Variant #21	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-666	Malicious File Transfer - UNC3313, Download, Variant #22	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-667	Malicious File Transfer - UNC3313, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-668	Malicious File Transfer - UNC3313, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-669	Malicious File Transfer - UNC3313, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-670	Malicious File Transfer - UNC3313, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-671	Malicious File Transfer - UNC3313, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-672	Malicious File Transfer - UNC3313, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-673	Malicious File Transfer - UNC3313, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,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
A107-674	Malicious File Transfer - UNC3313, NABLE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NABLE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-675	Malicious File Transfer - UNC3313, NABLE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NABLE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-676	Malicious File Transfer - UNC3313, NABLE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NABLE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-677	Malicious File Transfer - UNC3313, NABLE, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NABLE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-678	Malicious File Transfer - UNC3313, NABLE, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NABLE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-679	Malicious File Transfer - UNC3313, NABLE, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NABLE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-680	Malicious File Transfer - UNC3313, OPENGAZE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:OPENGAZE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-681	Malicious File Transfer - UNC3313, OPENGAZE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:OPENGAZE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-682	Malicious File Transfer - UNC3313, OPENGAZE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:OPENGAZE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-683	Malicious File Transfer - UNC3313, SCREENCONNECT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SCREENCONNECT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-684	Malicious File Transfer - UNC3313, SCREENCONNECT, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SCREENCONNECT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-685	Malicious File Transfer - UNC3313, SWANSOUL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SWANSOUL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-686	Malicious File Transfer - UNC3313, SWANSOUL, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SWANSOUL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-687	Malicious File Transfer - UNC3313, SYNCRO, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SYNCRO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-688	Malicious File Transfer - UNC3313, SYNCRO, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SYNCRO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-689	Malicious File Transfer - UNC3313, SYNCRO, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SYNCRO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-690	Malicious File Transfer - UNC3313, SYNCRO, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SYNCRO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-691	Malicious File Transfer - UNC3313, SYNCRO, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SYNCRO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-692	Malicious File Transfer - UNC3313, SYNCRO, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SYNCRO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-693	Malicious File Transfer - UNC3313, SYNCRO, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3313,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SYNCRO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-694	Malicious File Transfer - UNC5667, DCPHOENIX, PROTONGLOW, SILVERLIME, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DCPHOENIX,Malware:PROTONGLOW,Malware:SILVERLIME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-695	Malicious File Transfer - UNC5667, DCPHOENIX, PROTONGLOW, SILVERLIME, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DCPHOENIX,Malware:PROTONGLOW,Malware:SILVERLIME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-696	Malicious File Transfer - UNC5667, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-697	Malicious File Transfer - UNC5667, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-698	Malicious File Transfer - UNC5667, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,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
A107-699	Malicious File Transfer - UNC5667, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-700	Malicious File Transfer - UNC5667, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-701	Malicious File Transfer - UNC5667, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-702	Malicious File Transfer - UNC5667, Download, Variant #15	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-703	Malicious File Transfer - UNC5667, Download, Variant #16	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-704	Malicious File Transfer - UNC5667, Download, Variant #17	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-705	Malicious File Transfer - UNC5667, Download, Variant #18	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-706	Malicious File Transfer - UNC5667, Download, Variant #19	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-707	Malicious File Transfer - UNC5667, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-708	Malicious File Transfer - UNC5667, Download, Variant #20	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,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
A107-709	Malicious File Transfer - UNC5667, Download, Variant #21	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-710	Malicious File Transfer - UNC5667, Download, Variant #22	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-711	Malicious File Transfer - UNC5667, Download, Variant #23	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-712	Malicious File Transfer - UNC5667, Download, Variant #24	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-713	Malicious File Transfer - UNC5667, Download, Variant #25	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-714	Malicious File Transfer - UNC5667, Download, Variant #26	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-715	Malicious File Transfer - UNC5667, Download, Variant #27	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-716	Malicious File Transfer - UNC5667, Download, Variant #28	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-717	Malicious File Transfer - UNC5667, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-718	Malicious File Transfer - UNC5667, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,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
A107-719	Malicious File Transfer - UNC5667, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-720	Malicious File Transfer - UNC5667, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-721	Malicious File Transfer - UNC5667, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-722	Malicious File Transfer - UNC5667, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-723	Malicious File Transfer - UNC5667, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-724	Malicious File Transfer - UNC5667, FRONTLOAD, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FRONTLOAD,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-725	Malicious File Transfer - UNC5667, FRONTLOAD, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FRONTLOAD,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-726	Malicious File Transfer - UNC5667, GLOWSTICK, PROTONGLOW, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GLOWSTICK,Malware:PROTONGLOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-727	Malicious File Transfer - UNC5667, GLOWSTICK, PROTONGLOW, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GLOWSTICK,Malware:PROTONGLOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-728	Malicious File Transfer - UNC5667, GREYBAG, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYBAG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-729	Malicious File Transfer - UNC5667, GREYBAG, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYBAG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-730	Malicious File Transfer - UNC5667, GREYBAG, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYBAG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-731	Malicious File Transfer - UNC5667, GREYBAG, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYBAG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-732	Malicious File Transfer - UNC5667, GREYMIRROR, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYMIRROR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-733	Malicious File Transfer - UNC5667, GREYMIRROR, HORSESHOE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYMIRROR,Malware:HORSESHOE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-734	Malicious File Transfer - UNC5667, GREYMIRROR, PROTONGLOW, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYMIRROR,Malware:PROTONGLOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-735	Malicious File Transfer - UNC5667, GREYMIRROR, PROTONGLOW, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYMIRROR,Malware:PROTONGLOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-736	Malicious File Transfer - UNC5667, GREYMIRROR, PROTONGLOW, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYMIRROR,Malware:PROTONGLOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-737	Malicious File Transfer - UNC5667, GREYMIRROR, PROTONGLOW, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYMIRROR,Malware:PROTONGLOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-738	Malicious File Transfer - UNC5667, GREYMIRROR, PROTONGLOW, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYMIRROR,Malware:PROTONGLOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-739	Malicious File Transfer - UNC5667, GREYMIRROR, PROTONGLOW, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYMIRROR,Malware:PROTONGLOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-740	Malicious File Transfer - UNC5667, GREYMIRROR, PROTONGLOW, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYMIRROR,Malware:PROTONGLOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-741	Malicious File Transfer - UNC5667, GREYSHOT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYSHOT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-742	Malicious File Transfer - UNC5667, HORSESHOE, Download, Variant #1	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
A107-743	Malicious File Transfer - UNC5667, HORSESHOE, Download, Variant #2	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

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-744	Malicious File Transfer - UNC5667, HORSESHOE, Download, Variant #3	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
A107-745	Malicious File Transfer - UNC5667, HORSESHOE, Download, Variant #4	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
A107-746	Malicious File Transfer - UNC5667, HORSESHOE, Download, Variant #5	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
A107-747	Malicious File Transfer - UNC5667, HORSESHOE, Download, Variant #6	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
A107-748	Malicious File Transfer - UNC5667, HORSESHOE, Download, Variant #7	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
A107-749	Malicious File Transfer - UNC5667, HORSESHOE, Download, Variant #8	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
A107-750	Malicious File Transfer - UNC5667, IVYPHOENIX, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:IVYPHOENIX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-751	Malicious File Transfer - UNC5667, IVYPHOENIX, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:IVYPHOENIX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-752	Malicious File Transfer - UNC5667, LIGHTPHOENIX, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,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
A107-753	Malicious File Transfer - UNC5667, LIGHTPHOENIX, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTPHOENIX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-754	Malicious File Transfer - UNC5667, LIGHTPHOENIX, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTPHOENIX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-755	Malicious File Transfer - UNC5667, LIGHTPHOENIX, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTPHOENIX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-756	Malicious File Transfer - UNC5667, LIGHTPHOENIX, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTPHOENIX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-757	Malicious File Transfer - UNC5667, LIGHTPHOENIX, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTPHOENIX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-758	Malicious File Transfer - UNC5667, LIGHTPHOENIX, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTPHOENIX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-759	Malicious File Transfer - UNC5667, LIGHTPHOENIX, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTPHOENIX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-760	Malicious File Transfer - UNC5667, NULLCANVAS, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NULLCANVAS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-761	Malicious File Transfer - UNC5667, POTATOWALL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POTATOWALL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-762	Malicious File Transfer - UNC5667, POTATOWALL, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POTATOWALL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-763	Malicious File Transfer - UNC5667, POTATOWALL, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POTATOWALL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-764	Malicious File Transfer - UNC5667, POTATOWALL, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POTATOWALL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-765	Malicious File Transfer - UNC5667, PROTONGLOW, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PROTONGLOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-766	Malicious File Transfer - UNC5667, PROTONGLOW, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PROTONGLOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-767	Malicious File Transfer - UNC5667, PROTONGLOW, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PROTONGLOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-768	Malicious File Transfer - UNC5667, PROTONGLOW, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PROTONGLOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-769	Malicious File Transfer - UNC5667, PROTONGLOW, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PROTONGLOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-770	Malicious File Transfer - UNC5667, PROTONGLOW, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PROTONGLOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-771	Malicious File Transfer - UNC5667, ROADSIGN, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ROADSIGN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-772	Malicious File Transfer - UNC5667, ROADSIGN, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ROADSIGN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-773	Malicious File Transfer - UNC5667, ROADSIGN, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ROADSIGN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-774	Malicious File Transfer - UNC5667, ROADSIGN, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ROADSIGN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-775	Malicious File Transfer - UNC5667, ROADSIGN, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ROADSIGN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-776	Malicious File Transfer - UNC5667, ROADSIGN, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ROADSIGN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-777	Malicious File Transfer - UNC5667, ROADSIGN, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ROADSIGN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-778	Malicious File Transfer - UNC5667, ROADSIGN, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ROADSIGN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-779	Malicious File Transfer - UNC5667, ROADSIGN, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ROADSIGN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-780	Malicious File Transfer - UNC5667, ROADSIGN, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ROADSIGN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-781	Malicious File Transfer - UNC5667, RUBBERAXE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:RUBBERAXE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-782	Malicious File Transfer - UNC5667, RUBBERAXE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:RUBBERAXE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-783	Malicious File Transfer - UNC5667, RUBBERAXE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:RUBBERAXE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-784	Malicious File Transfer - UNC5667, RUBBERAXE, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:RUBBERAXE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-785	Malicious File Transfer - UNC5667, RUBBERAXE, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:RUBBERAXE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-786	Malicious File Transfer - UNC5667, RUBBERAXE, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:RUBBERAXE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-787	Malicious File Transfer - UNC5667, RUBBERAXE, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:RUBBERAXE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-788	Malicious File Transfer - UNC5667, SILVERLIME, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SILVERLIME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-789	Malicious File Transfer - UNC5667, SILVERLIME, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SILVERLIME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-790	Malicious File Transfer - UNC5667, SOFTMETAL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SOFTMETAL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-791	Malicious File Transfer - UNC5866, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5866,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-792	Malicious File Transfer - UNC5866, SACREDDESK, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5866,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SACREDDESK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-793	Malicious File Transfer - UNC5866, SACREDDESK, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5866,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SACREDDESK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-794	Malicious File Transfer - UNC5866, SACREDDESK, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5866,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SACREDDESK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-795	Malicious File Transfer - UNC5866, SACREDGAME, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5866,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SACREDGAME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-796	Malicious File Transfer - UNC5866, SACREDGAME, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5866,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SACREDGAME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-797	Malicious File Transfer - UNC5866, SACREDGAME, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5866,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SACREDGAME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-798	Malicious File Transfer - UNC5866, SACREDGAME, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5866,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SACREDGAME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-799	Malicious File Transfer - UNC6085, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-800	Malicious File Transfer - UNC6085, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-801	Malicious File Transfer - UNC6085, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-802	Malicious File Transfer - UNC6085, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,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
A107-803	Malicious File Transfer - UNC6085, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-804	Malicious File Transfer - UNC6085, HEAVYGRAM, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HEAVYGRAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-805	Malicious File Transfer - UNC6085, HEAVYGRAM, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HEAVYGRAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-806	Malicious File Transfer - UNC6085, HEAVYGRAM, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HEAVYGRAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-807	Malicious File Transfer - UNC6085, HEAVYGRAM, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HEAVYGRAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-808	Phishing Email - Malicious Link, APT42, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:APT42,Control:Email,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A107-809	Phishing Email - Malicious Link, UNC3313, SWANSOUL, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC3313,Control:Email,Malware:SWANSOUL,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A107-810	Phishing Email - Malicious Link, UNC5667, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC5667,Control:Email,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A107-811	Phishing Email - Malicious Link, UNC5970, Variant #1	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

Host CLI Actions

VID	Name	Tags

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-554	Host CLI - Create and Start Persistence Service FEfKS, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC5866,CWE:284,Control:Endpoint,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-555	Host CLI - TRUFFLEHOG Credential Harvesting from Code Repository, Variant #1	ATT&CK:Collection,ATT&CK:M1017,ATT&CK:M1018,ATT&CK:M1032,ATT&CK:M1047,ATT&CK:T1213.003,Actor:UNC1549,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-556	Host CLI - UNC1549, Create Local User with net1.exe, Variant #1	ATT&CK:M1026,ATT&CK:M1032,ATT&CK:Persistence,ATT&CK:T1136.001,Actor:UNC1549,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,Src:Internal:Trusted
A107-557	Host CLI - UNC1549, MINIJUNK, TWOSTROKE, Staging Files for Exfiltration, Variant #1	ATT&CK:Collection,ATT&CK:M1057,ATT&CK:T1005,Actor:UNC1549,CWE:200,Control:Endpoint,Malware:MINIJUNK,Malware:TWOSTROKE,NIST:AC-23,NIST:AC-4,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
A107-558	Host CLI - UNC1549, Reset Computer Account Password, Variant #1	ATT&CK:Credential Access,ATT&CK:M1015,ATT&CK:M1026,ATT&CK:M1027,ATT&CK:T1003.006,Actor:UNC1549,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
A107-559	Host CLI - UNC3313, SWANSOUL, Persistence via Run Key, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC3313,Control:Endpoint,Malware:SWANSOUL,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-560	Host CLI - UNC5667, ROADSIGN, Persistence via File Association Hijack, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1546.001,Actor:UNC3313,Actor:UNC5667,Control:Endpoint,Malware:ROADSIGN,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-561	Host CLI - UNC5667, STAGEHAND, Self Deletion Via Ping Command, Variant #1	ATT&CK:Defense Evasion,ATT&CK:T1070.004,Actor:UNC5667,Control:Endpoint,Malware:STAGEHAND,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-562	Host CLI - UNC6085, FOUDRE, Create Registry Key Artifact, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1024,ATT&CK:Persistence,ATT&CK:T1112,Actor:UNC6085,CWE:15,CWE:732,Control:Endpoint,Malware:FOUDRE,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-563	Host CLI - UNC6085, HEAVYGRAM, Enumerates Startup Items with WMIC, Variant #1	ATT&CK:Execution,ATT&CK:M1018,ATT&CK:M1026,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1047,Actor:UNC6085,Control:Endpoint,Malware:HEAVYGRAM,NIST:AC-17,NIST:CM-11,NIST:CM-7,NIST:IA-2,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-564	Host CLI - UNC6085, PAPERWRAP, WMI Reconnaissance, Variant #1	ATT&CK:Execution,ATT&CK:M1018,ATT&CK:M1026,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1047,Actor:UNC6085,Control:Endpoint,Malware:PAPERWRAP,NIST:AC-17,NIST:CM-11,NIST:CM-7,NIST:IA-2,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

Protected Theater Actions

VID	Name	Tags
A107-812	Protected Theater - APT42, SOSHISMITH, Embedded LNK Payload, Variant #1	ATT&CK:Execution,ATT&CK:M1018,ATT&CK:M1021,ATT&CK:M1026,ATT&CK:M1033,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1047,ATT&CK:M1049,ATT&CK:T1059,Actor:APT42,Control:Endpoint,Malware:SOSHISMITH,NIST:CM-11,OS:Windows:10,OS:Windows:11,RunAs:Admin,Src:Internal:Trusted
A107-813	Protected Theater - APT42, SOSHISMITH, Embedded LNK Payload, Variant #2	ATT&CK:Execution,ATT&CK:M1018,ATT&CK:M1021,ATT&CK:M1026,ATT&CK:M1033,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1047,ATT&CK:M1049,ATT&CK:T1059,Actor:APT42,Control:Endpoint,Malware:SOSHISMITH,NIST:CM-11,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-814	Protected Theater - APT42, VBS Downloader Network Beacon, Variant #1	ATT&CK:Execution,ATT&CK:M1021,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:M1042,ATT&CK:M1049,ATT&CK:T1059.005,Actor:APT42,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
A107-815	Protected Theater - CRUDEEXCLUDE, Impair Defenses via Defender Exclusion, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.001,Actor:UNC6085,CWE:284,Control:Endpoint,Malware:CRUDEEXCLUDE,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-816	Protected Theater - UNC1549, Clear RDP History Saved Servers, Variant #1	ATT&CK:Defense Evasion,ATT&CK:T1070.004,Actor:UNC1549,Control:Endpoint,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,Src:Internal:Trusted
A107-817	Protected Theater - UNC1549, Create Masqueraded Local Account, Variant #1	ATT&CK:M1026,ATT&CK:M1032,ATT&CK:Persistence,ATT&CK:T1136.001,Actor:UNC1549,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
A107-818	Protected Theater - UNC1549, CREDSTROKE, Execution, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1050,ATT&CK:T1218.011,Actor:UNC1549,CWE:114,Control:Endpoint,Malware:CREDSTROKE,NIST:CM-11,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
A107-819	Protected Theater - UNC1549, CREDSTROKE, Execution, Variant #2	ATT&CK:Defense Evasion,ATT&CK:M1050,ATT&CK:T1218.011,Actor:UNC1549,CWE:114,Control:Endpoint,Malware:CREDSTROKE,NIST:CM-11,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
A107-820	Protected Theater - UNC1549, POLARDROP, Executes Dropper to Drop Malicious DLL, 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,Actor:UNC1549,CWE:114,CWE:427,Control:Endpoint,Malware:POLARDROP,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
A107-822	Protected Theater - UNC1549, POLARDROP, 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:UNC1549,Control:Endpoint,Malware:POLARDROP,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
A107-823	Protected Theater - UNC1549, POLLREGISTER, Execution, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1050,ATT&CK:T1218.011,Actor:UNC1549,CWE:114,Control:Endpoint,Malware:POLLREGISTER,NIST:CM-11,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
A107-824	Protected Theater - UNC1549, TWOSTROKE, Component Drop, 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,Actor:UNC1549,CWE:114,CWE:427,Control:Endpoint,Malware:TWOSTROKE,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
A107-825	Protected Theater - UNC1549, TWOSTROKE, DLL Sideloading, 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,Actor:UNC1549,CWE:114,CWE:427,Control:Endpoint,Malware:TWOSTROKE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-829	Protected Theater - UNC1549, TWOSTROKE, Execution, Variant #11	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC1549,Control:Endpoint,Malware:TWOSTROKE,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
A107-832	Protected Theater - UNC1549, TWOSTROKE, Execution, Variant #5	ATT&CK:Defense Evasion,ATT&CK:M1050,ATT&CK:T1218.011,Actor:UNC1549,CWE:114,Control:Endpoint,Malware:TWOSTROKE,NIST:CM-11,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
A107-833	Protected Theater - UNC1549, TWOSTROKE, Execution, Variant #6	ATT&CK:Defense Evasion,ATT&CK:M1038,ATT&CK:M1044,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1574.001,Actor:UNC1549,CWE:114,CWE:427,Control:Endpoint,Malware:TWOSTROKE,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
A107-834	Protected Theater - UNC1549, TWOSTROKE, Execution, Variant #7	ATT&CK:Defense Evasion,ATT&CK:M1038,ATT&CK:M1044,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1574.001,Actor:UNC1549,CWE:114,CWE:427,Control:Endpoint,Malware:TWOSTROKE,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,Src:Internal:Trusted
A107-835	Protected Theater - UNC1549, TWOSTROKE, Execution, Variant #8	ATT&CK:Defense Evasion,ATT&CK:M1038,ATT&CK:M1044,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1574.001,Actor:UNC1549,CWE:114,CWE:427,Control:Endpoint,Malware:TWOSTROKE,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
A107-837	Protected Theater - UNC1549, TWOSTROKE, 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:UNC1549,Control:Endpoint,Malware:TWOSTROKE,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-839	Protected Theater - UNC3313, ATERA, Execution, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC3313,Control:Endpoint,Malware:ATERA,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-841	Protected Theater - UNC3313, ATERA, Execution, Variant #3	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC3313,Control:Endpoint,Malware:ATERA,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-842	Protected Theater - UNC3313, ATERA, Execution, Variant #4	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC3313,Control:Endpoint,Malware:ATERA,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-844	Protected Theater - UNC3313, NABLE, Installs RMM Agent, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:M1037,ATT&CK:M1038,ATT&CK:T1219,Actor:UNC3313,Control:Endpoint,Malware:NABLE,NIST:AC-17,NIST:AC-3,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-846	Protected Theater - UNC3313, OPENGAZE, Execution, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC3313,Control:Endpoint,Malware:OPENGAZE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-847	Protected Theater - UNC3313, PDQ, Connect Agent MSI Installation, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC3313,CWE:284,Control:Endpoint,Malware:PDQ,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-849	Protected Theater - UNC3313, PDQ, Install Connect Agent via MSI, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC3313,Control:Endpoint,Malware:PDQ,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-850	Protected Theater - UNC3313, PDQ, Installs MSI Package Portal.msi, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1026,ATT&CK:M1042,ATT&CK:T1218.007,Actor:UNC3313,Control:Endpoint,Malware:PDQ,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-851	Protected Theater - UNC3313, PDQ, Service Creation for Persistence, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC3313,CWE:284,Control:Endpoint,Malware:PDQ,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-852	Protected Theater - UNC3313, SWANSOUL, Execution, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC3313,Control:Endpoint,Malware:SWANSOUL,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-858	Protected Theater - UNC5667, GREYBAG, Execution, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,Control:Endpoint,Malware:GREYBAG,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-859	Protected Theater - UNC5667, GREYMIRROR, HORSESHOE, POTATOWALL, Registry Run Key for, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC5667,Control:Endpoint,Malware:GREYMIRROR,Malware:HORSESHOE,Malware:POTATOWALL,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-860	Protected Theater - UNC5667, GREYMIRROR, PROTONGLOW, Creates Service, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC5667,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
A107-861	Protected Theater - UNC5667, GREYMIRROR, PROTONGLOW, Drops Backdoor, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5667,Control:Endpoint,Malware:GREYMIRROR,Malware:PROTONGLOW,NIST:CM-7,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-862	Protected Theater - UNC5667, GREYMIRROR, PROTONGLOW, Drops Via Malicious Document, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,Control:Endpoint,Malware:GREYMIRROR,Malware:PROTONGLOW,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-863	Protected Theater - UNC5667, GREYMIRROR, PROTONGLOW, Execution, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,Control:Endpoint,Malware:GREYMIRROR,Malware:PROTONGLOW,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-864	Protected Theater - UNC5667, GREYSHOT, Executes to Connect to C2, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:M1037,ATT&CK:T1071,Actor:UNC5667,Control:Endpoint,Malware:GREYSHOT,NIST:AC-17,NIST:CM-7,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-865	Protected Theater - UNC5667, HORSESHOE, Drops SystemProc.exe, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1038,ATT&CK:M1045,ATT&CK:T1036.005,Actor:UNC5667,Control:Endpoint,Malware:HORSESHOE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-866	Protected Theater - UNC5667, HORSESHOE, File Move for Persistence, Variant #1	ATT&CK:Defense Evasion,ATT&CK:T1564.001,Actor:UNC5667,Control:Endpoint,Malware:HORSESHOE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-867	Protected Theater - UNC5667, HORSESHOE, Registry Persistence, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC5667,Control:Endpoint,Malware:HORSESHOE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-869	Protected Theater - UNC5667, LIGHTPHOENIX, Beacons to C2, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5667,Control:Endpoint,Malware:LIGHTPHOENIX,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-870	Protected Theater - UNC5667, LIGHTPHOENIX, Beacons to C2, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5667,Control:Endpoint,Malware:LIGHTPHOENIX,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-871	Protected Theater - UNC5667, LIGHTPHOENIX, Drops Burn.exe, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,Control:Endpoint,Malware:LIGHTPHOENIX,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-872	Protected Theater - UNC5667, LIGHTPHOENIX, Execution, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,Control:Endpoint,Malware:LIGHTPHOENIX,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-873	Protected Theater - UNC5667, LIGHTPHOENIX, File Drop, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC5667,Control:Endpoint,Malware:LIGHTPHOENIX,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-875	Protected Theater - UNC5667, Malicious Document Execution, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-878	Protected Theater - UNC5667, ROADSIGN, Executes Malicious Word Document, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,Control:Endpoint,Malware:ROADSIGN,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-879	Protected Theater - UNC5667, ROADSIGN, Execution, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,Control:Endpoint,Malware:ROADSIGN,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-880	Protected Theater - UNC5667, ROADSIGN, Execution, Variant #2	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,Control:Endpoint,Malware:ROADSIGN,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-881	Protected Theater - UNC5667, ROADSIGN, Execution, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5667,Control:Endpoint,Malware:ROADSIGN,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-882	Protected Theater - UNC5667, RUBBERAXE, Execution, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5667,Control:Endpoint,Malware:RUBBERAXE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-883	Protected Theater - UNC5667, RUBBERAXE, Execution, Variant #2	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,Control:Endpoint,Malware:RUBBERAXE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-884	Protected Theater - UNC5667, RUBBERAXE, Malicious Document Execution, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5667,Control:Endpoint,Malware:RUBBERAXE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-885	Protected Theater - UNC5667, RUBBERAXE, 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,Control:Endpoint,Malware:RUBBERAXE,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-886	Protected Theater - UNC5667, 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,ATT&CK:T1053.005: Scheduled Task/Job: Scheduled Task,Actor:UNC5667,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-889	Protected Theater - UNC5866, SACREDDESK, 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:UNC5866,Control:Endpoint,Malware:SACREDDESK,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-890	Protected Theater - UNC6085, BADMOVIE, Creates Run key Persistence, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC6085,Control:Endpoint,Malware:BADMOVIE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-891	Protected Theater - UNC6085, BADMOVIE, HTA Execution, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,Control:Endpoint,Malware:BADMOVIE,NIST:CM-7,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-892	Protected Theater - UNC6085, BADMOVIE, Initial Execution and Download, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6085,Control:Endpoint,Malware:BADMOVIE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-893	Protected Theater - UNC6085, CRUDEEXCLUDE, Add Defender Exclusion for MicrosoftDistribution, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.001,Actor:UNC6085,CWE:284,Control:Endpoint,Malware:CRUDEEXCLUDE,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-894	Protected Theater - UNC6085, CRUDEEXCLUDE, Add Defender Exclusion for ProgramData, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.001,Actor:UNC6085,CWE:284,Control:Endpoint,Malware:CRUDEEXCLUDE,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-895	Protected Theater - UNC6085, CRUDEEXCLUDE, Add Defender Exclusion for ZlibDate, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.001,Actor:UNC6085,CWE:284,Control:Endpoint,Malware:CRUDEEXCLUDE,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-896	Protected Theater - UNC6085, FOUDRE, SFXRAR, Create Scheduled Task via XML, 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:UNC6085,Control:Endpoint,Malware:FOUDRE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-897	Protected Theater - UNC6085, FOUDRE, SFXRAR, Dropper Execution, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6085,Control:Endpoint,Malware:FOUDRE,Malware:SFXRAR,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-898	Protected Theater - UNC6085, FOUDRE, SFXRAR, Executes SFX RAR to drop DLL, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6085,Control:Endpoint,Malware:FOUDRE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-899	Protected Theater - UNC6085, FOUDRE, SFXRAR, Scheduled Task (LicensingDiagSpp), 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:UNC6085,Control:Endpoint,Malware:FOUDRE,Malware:SFXRAR,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-900	Protected Theater - UNC6085, HEAVYGRAM, Add SMQDServicePackages to Defender Exclusions, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.001,Actor:UNC6085,CWE:284,Control:Endpoint,Malware:HEAVYGRAM,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-901	Protected Theater - UNC6085, HEAVYGRAM, Add Sysmain to Defender Exclusions, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.001,Actor:UNC6085,CWE:284,Control:Endpoint,Malware:HEAVYGRAM,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-902	Protected Theater - UNC6085, HEAVYGRAM, Add Windows Defender Exclusion, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.001,Actor:UNC6085,CWE:284,Control:Endpoint,Malware:HEAVYGRAM,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-903	Protected Theater - UNC6085, HEAVYGRAM, Creates Scheduled Task for Persistence, Variant #1	ATT&CK:Execution,ATT&CK:M1018,ATT&CK:M1026,ATT&CK:M1028,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1053.005,Actor:UNC6085,Control:Endpoint,Malware:HEAVYGRAM,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-904	Protected Theater - UNC6085, HEAVYGRAM, Drops a Malicious ZIP Archive, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,Control:Endpoint,Malware:HEAVYGRAM,NIST:CM-7,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-905	Protected Theater - UNC6085, HEAVYGRAM, Establishes Persistence via Registry Run Key, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC6085,Control:Endpoint,Malware:HEAVYGRAM,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-906	Protected Theater - UNC6085, HEAVYGRAM, Establishes 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:UNC6085,Control:Endpoint,Malware:HEAVYGRAM,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-907	Protected Theater - UNC6085, HEAVYGRAM, Establishes 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:UNC6085,Control:Endpoint,Malware:HEAVYGRAM,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-908	Protected Theater - UNC6085, HEAVYGRAM, 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:UNC6085,Control:Endpoint,Malware:HEAVYGRAM,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-909	Protected Theater - UNC6085, HEAVYGRAM, Sideloading Prep via Directory with Trailing Space, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1017,ATT&CK:M1022,ATT&CK:M1028,ATT&CK:M1038,ATT&CK:M1045,ATT&CK:T1036,Actor:UNC6085,CWE:706,Control:Endpoint,Malware:HEAVYGRAM,NIST:AC-4,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-910	Protected Theater - UNC6085, LIGHTMASS, Takes Screenshot via PowerShell, Variant #1	ATT&CK:Collection,ATT&CK:T1113,Actor:UNC6085,Control:Endpoint,Malware:LIGHTMASS,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

New Files

A total of 231 new files have been added to the File Library with this update. This includes 231 malicious files.

Malicious Files

File MD5	Tags

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
0043634018d17cac17df7052df12adc2	Group:Validation
05153410301cabd581f8697ea4653743	Malware:SACREDDESK,Group:Validation,Malware_Type:DATA_MINER
057e58ff00be3032fd6e3f5d2cc80905	Malware:RUBBERAXE,Malware_Type:BACKDOOR,Group:Validation
067922da3bd44493ffa74cbf880ad4a0	Group:Validation
06a2051cc476a806ce35d43efaf27b1c	Group:Validation
07502104c6884e6151f6e0a53966e199	Malware_Type:BACKDOOR,Group:Validation,Malware:POTATOWALL
0a01b11b2fa66e35c8b77844896b454b	Malware:SOFTMETAL,Group:Validation
0a656287defcbd8a9c47385b805993df	Group:Validation,Malware_Type:DOWNLOADER
0bb9432e088f2626195923e24d3c1cfe	Group:Validation,Malware:SFXRAR,Malware:FOUDRE,Malware_Type:DROPPER
0befbb6a14b3cbae42303a27bd06cad1	Group:Validation
0dfb603775ac520e3b6a441b9baa69be	Malware:ATERA,Group:Validation
10af4e0e90eb0ff371f32a049edc5511	Malware:LIGHTPHOENIX,Malware_Type:BACKDOOR,Group:Validation
10d25ef55824faee5adfc3fd6fa5f0db	Group:Validation,Malware:NABLE
11ee5f269902e37ab15e8ae2c5d37412	Malware:DCPHOENIX,Group:Validation,Malware_Type:DROPPER_MEMORY_ONLY
12af6d7eb20426e4e898273f45fc48aa	Malware:ATERA,Group:Validation
148ac56002d565184a65b24f61fe9273	Group:Validation,Malware:BADMOVIE,Malware_Type:DOWNLOADER
14d8e865d3ca67b88c01f7e5d2b0862d	Group:Validation,Malware:TWOSTROKE,Malware_Type:BACKDOOR
14fb6a186166577fab71d56cbe1c74d9	Group:Validation
16602375fc2dae1eb54580ab7eda6567	Group:Validation,Malware_Type:BACKDOOR,Malware:HEAVYGRAM
1679ab4099d4b886208d60f146cd4b91	Group:Validation
16dbb11d5c530e521593e06503a20722	Malware:TWOSTROKE,Malware_Type:BACKDOOR,Group:Validation
1874f341dbd074de3aefc0c58297f02a	Group:Validation,Malware:PROTONGLOW,Malware_Type:BACKDOOR

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
19427febf9f11f96d1d89a60da136de6	Group:Validation,Malware:TWOSTROKE,Malware_Type:BACKDOOR
1965a61d6f96b7bb221564ad52ba9719	Group:Validation,Malware:TWOSTROKE,Malware_Type:BACKDOOR
1b68bee0b72809d657ef40b947ca8c27	Malware_Type:BACKDOOR,Malware:SACREDGAME,Group:Validation
1baeff23794e47eb5c927c0303b7cd92	Malware_Type:BACKDOOR,Malware:TWOSTROKE,Group:Validation
1c8c4746a1669b00f53d846158dd9693	Malware:RUBBERAXE,Malware_Type:BACKDOOR,Group:Validation
1db9a657894cc0d78fe6f06ff614791f	Malware:NABLE,Group:Validation
1de19958e7c2ef14addfb35b43a594ec	Malware_Type:DROPPER_MEMORY_ONLY,Malware:PROTONGLOW,Group:Validation,Malware:GREYMIRROR
1e6b601f733bc40eaa58916986bfc5b9	Group:Validation,Malware_Type:BACKDOOR,Malware:HEAVYGRAM
1ef78a72e4957c04197992bab2f86335	Malware:NETSCAN,Group:Validation
1fbb089a4c0ac9c1e461323e75ba4fb2	Malware_Type:BACKDOOR,Malware:POTATOWALL,Group:Validation
20e80c787e129ec11de9accdd0ae4611	Group:Validation
223196939e1e1ba9256f515b0a510d7a	Group:Validation,Malware:TWOSTROKE,Malware_Type:BACKDOOR
227d4401b5e2436844f3deae7ca8ce5e	Group:Validation
24418a784989a4f615a4587f8492f1e1	Group:Validation,Malware_Type:BACKDOOR,Malware:MINIBIKE
24725e2759db07e879a6a0f248a4dc0b	Malware:LIGHTPHOENIX,Malware_Type:BACKDOOR,Group:Validation
26e5ff398ec6b30c51d6b6552bb932f8	Group:Validation
2956ec73ec77757271e612b81ca122c4	Group:Validation
29a06eb098d1c9cff91adfd0456649f9	Group:Validation
2a71cfe16028db4dcc29d4fae852a8be	Malware:LIGHTPHOENIX,Malware_Type:BACKDOOR,Group:Validation
2c19001d5b81037ac70ef17f887cbec0	Malware:LIGHTPHOENIX,Group:Validation,Malware_Type:BACKDOOR
2c630634721bbee199107cd4414da88b	Group:Validation,Malware:ATERA

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
2f2a7b00a4e9f4d22228de1ad41efa6d	Group:Validation
30689e455b6442355c656c9fa61f481f	Group:Validation
3106848925a39b9d51f9ad9f5963e417	Group:Validation,Malware:POLARDROP
32f51a376a8277649088047dd61efdf5	Malware:LIGHTPHOENIX,Malware_Type:BACKDOOR,Group:Validation
35f9dc1364f026e03153691c471174a8	Group:Validation
36d189f0c4bfbf573eb5c8a922755ab8	Group:Validation
36d83f11e6d66ecc44bedc1c51fadef5	Group:Validation,Malware:POLLREGISTER,Malware_Type:DROPPER
37b2836322db0dccef336de714e04d20	Group:Validation
3841c550816adb4be5726066ed7bf0fd	Group:Validation
384e118ce122574dab872efcbc2b222d	Group:Validation,Malware:RUBBERAXE,Malware_Type:BACKDOOR
38e20236b52ea7b5abed7168c0b1bd99	Malware:GREYBAG,Group:Validation,Malware_Type:DROPPER_MEMORY_ONLY
3a85381dd880c69f40b02859cd9fd473	Group:Validation,Malware:TWOSTROKE,Malware_Type:BACKDOOR
3a95186019af1943a0ea0f8eb07a288f	Malware_Type:DOWNLOADER,Group:Validation,Malware:ROADSIGN
3ab16bd1c339fd0727be650104b74dd1	Malware_Type:DROPPER_MEMORY_ONLY,Malware:PROTONGLOW,Group:Validation,Malware:GREYMIRROR
3b4eff3e22515fd1dac7ce0a91de1af7	Malware:SILVERLIME,Group:Validation,Malware_Type:LAUNCHER
3bb65d389d5c535f068328e607d2d688	Malware_Type:BACKDOOR,Malware:PROTONGLOW,Group:Validation
3c2fd296da55d1398edd7b6bb375a960	Group:Validation
3ca8a9ab86a5f8d42bdc49a80fc36de3	Group:Validation
3e935a07653db0f6e69fcd66d98acb09	Group:Validation,Malware_Type:BACKDOOR,Malware:HEAVYGRAM
3fddef610177acad4f69eee281894271	Group:Validation
409d02d6153af220e527fd72256ee3a5	Malware_Type:BACKDOOR,Group:Validation,Malware:HORSESHOE

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
41f4eb291cfbb3684a3cb98e55fd7e20	Malware:FRONTLOAD,Group:Validation,Malware_Type:BACKDOOR
42215c1fb55d945b4d2a0bb188ca4dcf	Group:Validation
4221ca1a9f9f6e0c9b9ddd58e2c2f863	Malware:SCREENCONNECT,Group:Validation
43c11ceaad7b30b7c73e0d15f78372b8	Group:Validation
46d8c2e72c49196781d2657e34cfe460	Group:Validation,Malware_Type:BACKDOOR,Malware:HEAVYGRAM
46e036b91e6673e3b46d43fb1e6d0104	Group:Validation,Malware_Type:BACKDOOR,Malware:SWANSOUL
482b0b4a853f35585d478d4b0e1373b8	Malware:SYNCRO,Group:Validation
4b555b3547b69aecf5bc87b97a857ed9	Malware:DCPHOENIX,Malware:PROTONGLOW,Malware:SILVERLIME,Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
4d5b14375f90a836e608c28491f0308b	Group:Validation
4dc1fa2fc3121e912736c727761c78d8	Group:Validation
4dee09dcd5ab407ee9086445303e7cdf	Malware_Type:DROPPER_MEMORY_ONLY,Malware:PROTONGLOW,Group:Validation,Malware:GLOWSTICK
53d0f4a75e8acbb6255bb44242e4843f	Malware:TWOSTROKE,Malware_Type:BACKDOOR,Group:Validation
561b2983d558283c446ff674ff6138c3	Group:Validation
575972fb4f2d0f59e9b4b63f7728cd75	Group:Validation,Malware:TWOSTROKE,Malware_Type:BACKDOOR
588467ebab23179620c45223d4f90a93	Group:Validation,Malware:SYNCRO
59247d7659ae0f65114a400eee390d26	Malware:SYNCRO,Group:Validation
5978579a37d9df72d4090f0ce90060a6	Group:Validation,Malware:TWOSTROKE,Malware_Type:BACKDOOR
5c8ec53a840f7d800f59e4e8253a398b	Malware_Type:BACKDOOR,Malware:OPENGAZE,Group:Validation
5e67d523f2a317dab4d5500f423bcb5b	Malware:SYNCRO,Group:Validation
5ec50bf344d45f6fb803fc0643feae23	Group:Validation
5fe1d97bc3ea66931fe0f588f0411c42	Malware_Type:DROPPER,Group:Validation,Malware:SFXRAR,Malware:FOUDRE

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
61eb76bd9a1638d3cf2886c8a626450a	Malware:SWANSOUL,Group:Validation,Malware_Type:BACKDOOR
62fbf0622586324f7177da466d036b8f	Group:Validation,Malware:POWERPUG
62fe0b98c11f76b5bb5619331a0aa386	Group:Validation
63f46ab9c3e4792e5e1d8ab0e56fe568	Group:Validation
64af4e6216026ed8fcfbf8b07ee20707	Malware_Type:BACKDOOR,Group:Validation,Malware:POTATOWALL
64e7e2d2e037d21e8564de52061a31c7	Malware_Type:BACKDOOR,Group:Validation,Malware:OPENGAZE
6636407299e0b1a74961ae998cec20e0	Malware_Type:DROPPER_MEMORY_ONLY,Malware:PROTONGLOW,Group:Validation,Malware:GLOWSTICK
67dbe102978e4b612237ad3ee371702f	Malware:TWOSTROKE,Malware_Type:BACKDOOR,Group:Validation
68aa683fc8522f0c354e53465f01f19e	Malware_Type:BACKDOOR,Malware:SACREDGAME,Group:Validation
6aaf7de557eb94a745432f2c2d0fa2bb	Group:Validation
6e08be92655237f4332d2172b464d36c	Malware:SACREDDESK,Group:Validation,Malware_Type:DATA_MINER
6e7eb2e602e95c6cdda4d9fdc673364c	Malware:ATERA,Group:Validation
70492bc160d0a7d47e8680fbbc87c76d	Group:Validation
7358d370afe6907f182b57e98e6920ad	Group:Validation
7391c3d895246dbd5d26bf70f1d8cbad	Group:Validation
74e75830252220cbbe7e3adec4340d2d	Malware_Type:DOWNLOADER,Group:Validation,Malware:ROADSIGN
78b778ba0bcd546337077a50b8f90532	Malware_Type:BACKDOOR,Malware:PROTONGLOW,Group:Validation
7bfbc76c7eeb652d73b85c99ee83b339	Group:Validation,Malware:HORSESHOE,Malware_Type:DROPPER_MEMORY_ONLY
7c039aa1bc6c5657d8cdf5f2983aea4f	Group:Validation
7d216c57da81193a45c67c323d4049c3	Malware_Type:BACKDOOR,Malware:TWOSTROKE,Group:Validation
7d5b1ae57599940faf51e0b38f4824bd	Malware:FRONTLOAD,Malware_Type:BACKDOOR,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
7e361ec597d5e0743ebd47a7e20dbc09	Group:Validation,Malware:ATERA
7e73ca410dc6480c77a9236c0733c0a1	Malware_Type:DROPPER_MEMORY_ONLY,Malware:PROTONGLOW,Group:Validation,Malware:GREYMIRROR
7ebea1328b6fe3751dd0250452c466ce	Malware:ATERA,Group:Validation
7f24a7a488dc2f26901342e5bd0b54d7	Group:Validation
83b7ec5f0d5d6f11ba1284a3f705e98e	Group:Validation,Malware:TWOSTROKE,Malware_Type:BACKDOOR
84534eeb7d5717020891839731c1ac49	Group:Validation,Malware_Type:BACKDOOR,Malware:FOUDRE
85a2dba599390143c665e349f9f04161	Malware:RUBBERAXE,Malware_Type:BACKDOOR,Group:Validation
87144d0aa002a87376b673f7d0c0eb88	Group:Validation,Malware_Type:INSTALLER,Malware:SOSHISMITH
886507333ed05dcf740ff903d6b455b7	Group:Validation
88e9acbc222b83d524dd4174367dec8b	Malware:RUBBERAXE,Malware_Type:BACKDOOR,Group:Validation
8e3654412f3b117264e48db0caa8ebf3	Group:Validation,Malware:ATERA
8e9e81d1b252d7fa99579e9cf2e4b4ba	Group:Validation
8eb107b3dde0a7ac039c668b427a3634	Group:Validation
8ec79493227de002cf623bca2d59c7a3	Group:Validation
928d521d903aa83d30368bd09aa8be18	Group:Validation
92a929096521990e3e03ebcceb3dc177	Group:Validation
92d497053600374b10003aa40ae8e5d8	Malware:POWERPUG,Group:Validation
92fc7724688108d3ad841f3d2ce19dc7	Group:Validation
932a43ae94b634836e0d6d13cfe740b0	Group:Validation
9359db7c6622e2eef2824c97c7916fec	Group:Validation
9550467f4b8415eee1650d243f92980e	Group:Validation
9601defda7127aedb6cd6fca7f6c6805	Group:Validation,Malware:SFXRAR,Malware_Type:DROPPER
968a57c20844e104d5b32628a8b40aaa	Malware:TWOSTROKE,Malware_Type:BACKDOOR,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
96a9078d97a8b2a0cdc6632b48b8a649	Malware_Type:BACKDOOR,Malware:TWOSTROKE,Group:Validation
9a1b964ff95a216cb3f66482b33a8af8	Group:Validation,Malware:POLLREGISTER,Malware_Type:BACKDOOR
9b01ccc5277c81b9178a41cbfbc8bb3e	Malware_Type:BACKDOOR,Malware:HEAVYGRAM,Group:Validation
9bdcaf0aac5e422c600d160cf01cca12	Group:Validation
9d0d2eab4e024ccd55c330ede36424aa	Group:Validation
9fa34dcdec188138ded6a48877076405	Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation,Malware:GREYMIRROR
a076f6e6782ec914df97500fb24914d7	Malware_Type:LAUNCHER,Group:Validation,Malware:NULLCANVAS
a1787fc51fea1b01ed72a7e19cc36bfc	Group:Validation,Malware:POLLREGISTER,Malware_Type:BACKDOOR
a17b40b8133c1cc29c6146732086db69	Group:Validation,Malware:TWOSTROKE,Malware_Type:BACKDOOR
a2522c16248868ad666c746baf428e41	Malware:POWERPUG,Group:Validation
a39f74247367e0891f18b7662c8e69b5	Group:Validation
a408e056425307096dbf3e8b50a0b673	Malware:GREYMIRROR,Malware_Type:DROPPER_MEMORY_ONLY,Malware:PROTONGLOW,Group:Validation
a4f6b56f41ddf762d9f1d9666c796c8b	Group:Validation,Malware:TWOSTROKE,Malware_Type:BACKDOOR
a52c8eacf3dbdcf0f49268a27a44636b	Group:Validation
a546d2363a4b94e361d0874b690c853b	Malware:LIGHTPHOENIX,Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
a8a5871db3217e394dd50d30eb2ea464	Group:Validation,Malware:LIGHTRAIL,Malware_Type:TUNNELER
a909cf434df9fc8ae10e33903fc38e1c	Group:Validation
a9235540208fa6a25614c24a59e19199	Malware_Type:DROPPER,Malware:HORSESHOE,Group:Validation
a9effec03c1945f791e72c39acf51f8f	Malware:GREYSHOT,Malware_Type:BACKDOOR,Group:Validation
aa38567e4d34bf4cec5635680e48b1b5	Malware:GREYBAG,Group:Validation,Malware_Type:DROPPER_MEMORY_ONLY

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
aa75a0baebc93d4ca7498453ef64128a	Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation,Malware:HORSESHOE,Malware:GREYMIRROR
adf7606b900fa1d4630f7fd63a585e60	Malware_Type:DROPPER_MEMORY_ONLY,Malware:DCPHOENIX,Malware:PROTONGLOW,Group:Validation,Malware:SILVERLIME
ae7a7a05afc09adb64d307fefe22ba86	Group:Validation
b15c11faf60a41f855e117d9c1886b92	Malware_Type:DOWNLOADER,Group:Validation,Malware:ROADSIGN
b19a097c237d594a85986881f69f127d	Malware:TWOSTROKE,Malware_Type:BACKDOOR,Group:Validation
b278f231ae7018c9d3aad61325ddc781	Group:Validation,Malware_Type:BACKDOOR,Malware:TWOSTROKE
b319d8972115895f156807348fa9b45f	Group:Validation,Malware:TWOSTROKE,Malware_Type:BACKDOOR
b35a291038aac657fd60118ef2b9af20	Group:Validation
b3c1a3eebefafe1346c6a864b5423182	Group:Validation,Malware:HEAVYGRAM,Malware_Type:DROPPER
b3d91aaccecb3647c518feec54758bc0	Group:Validation,Malware_Type:INSTALLER,Malware:FOUDRE
b4b673c0a60e57c9c8f7560d609902b6	Malware_Type:BACKDOOR,Malware:PROTONGLOW,Group:Validation
b4e817bd7119f93f7593fd63c3dee26d	Malware:POLLREGISTER,Malware_Type:DROPPER,Group:Validation
b638d6c0064d56c2bcb222f2327f5e1d	Malware:ATERA,Group:Validation
b74514081fd6a4d4c2b86c06ec16d9c5	Malware:ATERA,Group:Validation
b7e4b752adff07ac1b7b67a9be30b366	Malware_Type:BACKDOOR,Malware:TWOSTROKE,Group:Validation
b9399872373e921bcd189cd99eb0d033	Malware:POLLBLEND,Group:Validation,Malware_Type:TUNNELER
bafbb2bedb193b53bf053784a88768c0	Malware_Type:TUNNELER,Malware:POLLBLEND,Group:Validation
bb3587d3da3fbe4ab8c36721d9435327	Group:Validation
be83a1388c5734b16d5ff7a586906ab8	Group:Validation,Malware:BADMOVIE,Malware_Type:DOWNLOADER
bee36937d4cf029e38a3abb4343af46d	Malware:SCREENCONNECT,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
bf3d7de6fceaade9f45c667e91fe4f03	Group:Validation
c0ecdfcb960a63c94c936475d20d27ab	Group:Validation,Malware_Type:INSTALLER,Malware:FOUDRE
c0fad3bdb4d0bd55ac8966687cf7c8fa	Malware:LIGHTPHOENIX,Malware_Type:BACKDOOR,Group:Validation
c1225b502c387b6cb9b96ac0e6d9964c	Group:Validation
c192db3db7a8ec917fa791effe5b0b12	Malware:ATERA,Group:Validation
c2fd40817bfc98078cbb1246d269667c	Malware:SACREDDESK,Group:Validation,Malware_Type:DATA_MINER
c3b3f5eb407f8c3e1b69c60eead4f7dd	Malware:IVYPHOENIX,Group:Validation,Malware_Type:DOWNLOADER
c478e472f6223e7ee92cff8b459e55e2	Malware_Type:DOWNLOADER,Group:Validation,Malware:ROADSIGN
c48beca28da76f589ac9eb5b5f2df787	Group:Validation,Malware:SYNCRO
c5d2b7208e1ae3961ebd9484e5285988	Group:Validation,Malware_Type:BACKDOOR,Malware:HEAVYGRAM
c6fcc61eb707a95e6a83adf817d3d9a5	Group:Validation,Malware_Type:BACKDOOR,Malware:HEAVYGRAM
cbcf58588e8cc9f3edaac9493e6c3660	Group:Validation
cd0922a41668ffc59c7f311edf625d18	Group:Validation,Malware:ATERA
cd6e918bbcd562df59a563b68a82821c	Group:Validation
cdbe76cdfdec8f7c09781b2ef0fdb7f4	Group:Validation
ce2dd8e98cde74732fbeac6f953e9be0	Group:Validation
d067c3fff70c1d61b60f2409090caade	Malware:SILVERLIME,Malware_Type:DROPPER_MEMORY_ONLY,Malware:PROTONGLOW,Group:Validation,Malware:DCPHOENIX
d1af72a943f3b1eb45934e07f205c5ed	Malware_Type:DROPPER_MEMORY_ONLY,Malware:PROTONGLOW,Group:Validation,Malware:GREYMIRROR
d2b0785b69f8578bdddf039634507f47	Group:Validation
d5398df29c8873b690ee50da8ec815c9	Malware:TWOSTROKE,Group:Validation,Malware_Type:BACKDOOR
d6ad04612f9a6060f3955c43ad5cf236	Malware_Type:DROPPER_MEMORY_ONLY,Malware:PROTONGLOW,Malware:GREYMIRROR,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
d8e5abafabef3ff5e466d472f22cb855	Malware:ATERA,Group:Validation
d93562ef6487674c6a3442702be88f6b	Malware:ATERA,Group:Validation
d9619d23098231bec2f17787d1d1b182	Group:Validation,Malware_Type:DOWNLOADER,Malware:ROADSIGN
dd236996f30a2c1a6825ef855207fc4f	Group:Validation,Malware:HEAVYGRAM,Malware_Type:DROPPER
dd6af28d1a03193fc76001b04d5827cc	Malware:HORSESHOE,Group:Validation,Malware_Type:BACKDOOR
de51f9814b9b2a37e3189f1708a8ce1e	Malware:SYNCRO,Group:Validation
df3bbdab7542018b0141562061b2e16c	Group:Validation
e1e00d96bb2b4a82c4264738825814e0	Group:Validation,Malware:NABLE
e23637423599434a6de45b9080b7c561	Group:Validation,Malware:TWOSTROKE,Malware_Type:BACKDOOR
e2447ee6d2c9f9cd22d726f3a7a7823d	Group:Validation
e2a5019f85a8aed140b13c87cf9a791a	Malware_Type:BACKDOOR,Malware:PROTONGLOW,Group:Validation
e3ed457861e8930d04016d6c2eaeb9b1	Malware:ATERA,Group:Validation
e47b6ae23c3fcaf0b5df7773c8250692	Group:Validation
e52455d67d3d45211aae128bda4f57e9	Group:Validation,Malware:ATERA
e5dd608292b6f421b0c108816d25fc5e	Malware:HORSESHOE,Malware_Type:BACKDOOR,Group:Validation
e627eebb5acaa98fc10698c82f7ec300	Group:Validation,Malware:POTATOWALL,Malware_Type:BACKDOOR
e67672c927cab54ac39bef826c4228d2	Malware:SACREDDESK,Group:Validation,Malware_Type:DATA_MINER
e67c4eee0f424064d811794fc8f80130	Malware_Type:DOWNLOADER,Group:Validation,Malware:ROADSIGN
e68435f3899d0f01810afff7a420429f	Malware:GREYBAG,Group:Validation,Malware_Type:DROPPER_MEMORY_ONLY
e73ba93d008affdc4cce0cb4e18ae5c6	Malware_Type:DROPPER_MEMORY_ONLY,Malware:PROTONGLOW,Group:Validation,Malware:GREYMIRROR
e8e0f2ade7294808d86b23a989b21be1	Malware:TWOSTROKE,Malware_Type:BACKDOOR,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
edf07de9ebd4a4d6f82e6f4d7a01a959	Malware_Type:BACKDOOR,Malware:HEAVYGRAM,Group:Validation
f0376d225f450034e6b5ad29b196c76d	Group:Validation,Malware_Type:TUNNELER
f06e30dee8629e951cefa73373fdef9d	Malware_Type:DOWNLOADER,Group:Validation,Malware:ROADSIGN
f07edd187ba8cd83b98067c93ad6a8f1	Malware:GREYBAG,Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
f110ade78ed942a9f97d5551ca0ec562	Group:Validation,Malware:SYNCRO
f26de9d478c96df37e6f1d4c77d15dde	Group:Validation,Malware_Type:INSTALLER,Malware:SOSHISMITH
f34e0a09669ab007d3fd4bddfc9ec250	Group:Validation,Malware_Type:DOWNLOADER
f5ef5f40922113c2dfb32c202ae2b3f5	Malware:RUBBERAXE,Malware_Type:BACKDOOR,Group:Validation
f63ceb9f6b3a28b6858976e5549d3247	Group:Validation
f7101c581319fcd581f3045b5b7d6d09	Group:Validation,Malware_Type:BACKDOOR,Malware:HEAVYGRAM
f800f73cbbd71a1edf409364ed84abfa	Malware_Type:BACKDOOR,Malware:SACREDGAME,Group:Validation
f80c555be5e14cbf8c80c16f0eef358d	Malware_Type:BACKDOOR,Group:Validation
f97650ede0c39a29b0b5c5472f685d11	Group:Validation
fac805be171884ddbd1396f6a59c90eb	Group:Validation,Malware:TWOSTROKE,Malware_Type:BACKDOOR
fc3b282baa52ae723a8b0d038bc2c42e	Group:Validation
fc676435a6f39c244a03067944836045	Malware_Type:BACKDOOR,Malware:SACREDGAME,Group:Validation
fd75770a2ef293fe0c2ffe1c46cbd904	Group:Validation
fddb1bc970efa534278addc3913d89cf	Group:Validation
ff13ffc76bf452783fd74a74558a6cf4	Group:Validation,Malware:LIGHTMASS,Malware_Type:DOWNLOADER
ffd9c0245e68939549ce0e3a1e15fdb4	Malware:RUBBERAXE,Malware_Type:BACKDOOR,Group:Validation

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

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

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.