Mandiant

VHR20260401 - APRIL 1, 2026

The Mandiant Intelligence Validation Research Team (VRT) has published VHR20260401 - 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

- 171 Actions added
- 98 Files added
- 1 Action updated

Release Highlights

- A new Action covering **APT34** (https://advantage.mandiant.com/actors/APT34), an Iranian state-sponsored cyber espionage group operational since at least 2014, largely focused on phishing efforts to benefit Iranian nation-state interests.
- New Actions covering **UNC5187** (https://advantage.mandiant.com/actors/UNC5187), a suspected Iranian cyber espionage group with moderate-confidence ties to **APT34** (https://advantage.mandiant.com/actors/APT34) that primarily conducts malware deployment operations.
- New Actions covering **UNC5667** (https://advantage.mandiant.com/actors/UNC5667), a suspected subcluster of Iranian espionage actor **UNC3313** (https://advantage.mandiant.com/actors/UNC3313) that primarily conducts custom malware deployment operations via spearphishing against Israel-based organizations.
- A new Action demonstrating **Campaign 26-024** (https://advantage.mandiant.com/campaigns/CAMP.26.024), a suspected Iranian threat group **UNC6729** (https://advantage.mandiant.com/actors/UNC6729) campaign targeting Israeli citizens with **PANICPOACH** (https://advantage.mandiant.com/malware/PANICPOACH) Android malware.
- A new Action demonstrating **Campaign 26-027** (https://advantage.mandiant.com/campaigns/CAMP.26.027), a suspected Iranian espionage-motivated threat actor **UNC6085** (https://advantage.mandiant.com/actors/UNC6085) campaign that deploys custom backdoors and info-stealers via themed decoys and Telegram API C2.
- New Actions demonstrating **Campaign 26-021** (https://advantage.mandiant.com/campaigns/CAMP.26.021), an Iranian espionage group **UNC5866** (https://advantage.mandiant.com/actors/UNC5866) campaign conducting data mining and operational interference against suspected Israeli targets using **SACREDDESK** (https://advantage.mandiant.com/malware/SACREDDESK), **SACREDGAME** (https://advantage.mandiant.com/malware/SACREDGAME), and **SPACEHAMMER** (https://advantage.mandiant.com/malware/SPACEHAMMER) malware.
- New Actions demonstrating **Campaign 25-079** (https://advantage.mandiant.com/campaigns/CAMP.25.079), an actor **UNC6566** (https://advantage.mandiant.com/actors/UNC6566) campaign leveraging a supply chain compromise to distribute 'Shai-Hulud' NPM Worm and using **TRUFFLEHOG** (https://advantage.mandiant.com/malware/TRUFFLEHOG) to steal credentials.
- New Actions covering **Campaign 26-017** (https://advantage.mandiant.com/campaigns/CAMP.26.017), which details an actor of unknown motivations deploying malware via ClickFix lures with scheduled task persistence and Defender evasion.
- New Actions demonstrating **Campaign 26-019** (https://advantage.mandiant.com/campaigns/CAMP.26.019), a campaign by **UNC6572** (https://advantage.mandiant.com/actors/UNC6572) distributing **PALEKEY** (https://advantage.mandiant.com/malware/PALEKEY) and **DARKKEY** (https://advantage.mandiant.com/malware/DARKKEY.WINDOW) malware via fake installers.
- New Actions demonstrating **Campaign 26-013** (https://advantage.mandiant.com/campaigns/CAMP.26.013), a financially motivated threat group **UNC6692** (https://advantage.mandiant.com/actors/UNC6692) leveraging **SNOWBELT** (https://advantage.mandiant.com/malware/SNOWBELT), **SNOWGLAZE**

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

(https://advantage.mandiant.com/malware/SNOWGLAZE), and **SNOWBASIN** (https://advantage.mandiant.com/malware/SNOWBASIN) for browser-based access, network exploration, and data exfiltration via LimeWire API.

- A new Action covering **Campaign 26-016** (https://advantage.mandiant.com/campaigns/CAMP.26.016), a global cyber espionage campaign by PRC-nexus threat actor **UNC2814** (https://advantage.mandiant.com/actors/UNC2814) leveraging the **GRIDTIDE** (https://advantage.mandiant.com/malware/GRIDTIDE) backdoor to exfiltrate sensitive subscriber data and monitor private communications.

New Actions

A total of 171 Actions have been added to the content baseline with this update. This includes 131 Network Actions, 4 Host CLI Actions, and 36 Protected Theater Actions. All Actions in this release are tagged using the MITRE ATT&CK v17.1 framework.

Network Actions

VID	Name	Tags
A107-911	Command and Control - UNC5655, ERIESNAKE.GO, 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:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:ERIESNAKE.GO,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-912	Command and Control - UNC5655, NEATSNAKE, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:NEATSNAKE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-913	Command and Control - UNC5655, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1132.001,Actor:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-914	Command and Control - UNC5667, LIGHTPHOENIX, Check-In, Variant #2	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,GLOBAL.26.002,Malware:LIGHTPHOENIX,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-915	Command and Control - UNC5667, LIGHTPHOENIX, Registration, Variant #2	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,GLOBAL.26.002,Malware:LIGHTPHOENIX,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-916	Command and Control - UNC5667, LIGHTPHOENIX, Registration, Variant #3	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,GLOBAL.26.002,Malware:LIGHTPHOENIX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-917	Command and Control - UNC5795, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-918	Command and Control - UNC5795, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-920	Command and Control - UNC5795, Exfiltration, Variant #2	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-921	Command and Control - UNC5795, HOTAIR, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1567.002,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:HOTAIR,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-922	Command and Control - UNC5795, HOTAIR, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:HOTAIR,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-923	Command and Control - UNC5795, HOTAIR, Tasking, Variant #2	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102.001,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:HOTAIR,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-924	Command and Control - UNC5795, HOTAIR, Tasking, Variant #3	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:HOTAIR,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-925	Command and Control - UNC5795, HOTAIR, Tasking, Variant #4	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-926	Command and Control - UNC5795, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-927	Command and Control - UNC5795, TREEWORLD, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573.002,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:TREEWORLD,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-928	Command and Control - UNC5795, TREEWORLD, Check-In, Variant #2	ATT&CK:Command and Control,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:TREEWORLD,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-929	Command and Control - UNC5795, TREEWORLD, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:TREEWORLD,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-930	Command and Control - UNC5866, SACREDGAME, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5866,CAMP.26.021,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:SACREDGAME,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-931	Command and Control - UNC5866, SACREDGAME, Check-In, Variant #2	ATT&CK:Command and Control,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573.002,Actor:UNC5866,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,GLOBAL.26.002,Malware:SACREDGAME,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-932	Command and Control - UNC6085, Exfiltration, Variant #2	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,CAMP.26.027,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-934	Command and Control - UNC6085, LIGHTMASS, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6085,CAMP.26.027,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTMASS,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-935	Command and Control - UNC6085, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6085,CAMP.26.027,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-936	Command and Control - UNC6572, DUSTYKEY, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6572,CAMP.26.019,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTYKEY,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-937	Command and Control - UNC6572, DUSTYKEY, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,Actor:UNC6572,CAMP.26.019,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTYKEY,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-938	Command and Control - UNC6572, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1568,Actor:UNC6572,CAMP.26.019,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-939	Command and Control - UNC6713, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6713,CAMP.26.017,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-940	Command and Control - UNC6713, Check-In, Variant #2	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,Actor:UNC6713,CAMP.26.017,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-941	Command and Control - UNC6713, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6713,CAMP.26.017,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-942	Command and Control - UNC6713, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102.003,Actor:UNC6713,CAMP.26.017,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-947	Malicious File Transfer - REGALSPICE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REGALSPICE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-948	Malicious File Transfer - REGALSPICE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REGALSPICE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-949	Malicious File Transfer - UNC2814, GRIDTIDE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2814,CAMP.26.016,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GRIDTIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-950	Malicious File Transfer - UNC5187, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5187,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-951	Malicious File Transfer - UNC5187, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5187,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-952	Malicious File Transfer - UNC5187, ENDDOT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5187,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ENDDOT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-953	Malicious File Transfer - UNC5187, ENDDOT, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5187,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ENDDOT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-954	Malicious File Transfer - UNC5187, ENDDOT, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5187,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ENDDOT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-955	Malicious File Transfer - UNC5187, ENDDOT, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5187,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ENDDOT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-956	Malicious File Transfer - UNC5187, HOPEDFOR, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5187,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOPEDFOR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-957	Malicious File Transfer - UNC5187, HOPEDFOR, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5187,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOPEDFOR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-958	Malicious File Transfer - UNC5187, MAILDOT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5187,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MAILDOT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-959	Malicious File Transfer - UNC5187, MAILDOT, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5187,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MAILDOT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-960	Malicious File Transfer - UNC5187, SNARESEND, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5187,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SNARESEND,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-961	Malicious File Transfer - UNC5187, SPAREPRIZE, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5187,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SPAREPRIZE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-962	Malicious File Transfer - UNC5187, SPAREPRIZE, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5187,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SPAREPRIZE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-963	Malicious File Transfer - UNC5482, SPACENOISE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5482,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SPACENOISE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-964	Malicious File Transfer - UNC5482, SPACENOISE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5482,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SPACENOISE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-965	Malicious File Transfer - UNC5482, SPACENOISE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5482,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SPACENOISE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-966	Malicious File Transfer - UNC5655, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-967	Malicious File Transfer - UNC5655, ERIESNAKE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ERIESNAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-968	Malicious File Transfer - UNC5655, ERIESNAKE, ERIESNAKE.GO, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ERIESNAKE,Malware:ERIESNAKE.GO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-969	Malicious File Transfer - UNC5655, ERIESNAKE, ERIESNAKE.GO, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ERIESNAKE,Malware:ERIESNAKE.GO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-970	Malicious File Transfer - UNC5655, ERIESNAKE, ERIESNAKE.GO, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ERIESNAKE,Malware:ERIESNAKE.GO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-971	Malicious File Transfer - UNC5655, ERIESNAKE, ERIESNAKE.GO, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ERIESNAKE,Malware:ERIESNAKE.GO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-972	Malicious File Transfer - UNC5655, ERIESNAKE, ERIESNAKE.GO, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ERIESNAKE,Malware:ERIESNAKE.GO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-973	Malicious File Transfer - UNC5655, ERIESNAKE, ERIESNAKE.GO, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ERIESNAKE,Malware:ERIESNAKE.GO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-974	Malicious File Transfer - UNC5655, ERIESNAKE, ERIESNAKE.GO, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ERIESNAKE,Malware:ERIESNAKE.GO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-975	Malicious File Transfer - UNC5655, ERIESNAKE, ERIESNAKE.GO, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ERIESNAKE,Malware:ERIESNAKE.GO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-976	Malicious File Transfer - UNC5655, ERIESNAKE, ERIESNAKE.GO, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ERIESNAKE,Malware:ERIESNAKE.GO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-977	Malicious File Transfer - UNC5655, ERIESNAKE, ERIESNAKE.GO, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ERIESNAKE,Malware:ERIESNAKE.GO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-978	Malicious File Transfer - UNC5655, ERIESNAKE, ERIESNAKE.GO, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ERIESNAKE,Malware:ERIESNAKE.GO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-979	Malicious File Transfer - UNC5655, NEATSNAKE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5655,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEATSNAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-980	Malicious File Transfer - UNC5795, AEROSTAT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:AEROSTAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-981	Malicious File Transfer - UNC5795, CHISEL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CHISEL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-982	Malicious File Transfer - UNC5795, CHISEL, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CHISEL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-983	Malicious File Transfer - UNC5795, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-984	Malicious File Transfer - UNC5795, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-985	Malicious File Transfer - UNC5795, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-986	Malicious File Transfer - UNC5795, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-987	Malicious File Transfer - UNC5795, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-988	Malicious File Transfer - UNC5795, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-989	Malicious File Transfer - UNC5795, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,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
A107-990	Malicious File Transfer - UNC5795, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-991	Malicious File Transfer - UNC5795, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-992	Malicious File Transfer - UNC5795, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-993	Malicious File Transfer - UNC5795, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-994	Malicious File Transfer - UNC5795, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-995	Malicious File Transfer - UNC5795, HOTAIR, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-996	Malicious File Transfer - UNC5795, HOTAIR, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-997	Malicious File Transfer - UNC5795, HOTAIR, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A107-998	Malicious File Transfer - UNC5795, HOTAIR, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-999	Malicious File Transfer - UNC5795, HOTAIR, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-000	Malicious File Transfer - UNC5795, HOTAIR, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-001	Malicious File Transfer - UNC5795, HOTAIR, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-002	Malicious File Transfer - UNC5795, HOTAIR, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-003	Malicious File Transfer - UNC5795, HOTAIR, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-004	Malicious File Transfer - UNC5795, HOTAIR, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-005	Malicious File Transfer - UNC5795, HOTAIR, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-006	Malicious File Transfer - UNC5795, HOTAIR, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-007	Malicious File Transfer - UNC5795, HOTAIR, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-008	Malicious File Transfer - UNC5795, TREEWORLD, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TREEWORLD,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-009	Malicious File Transfer - UNC5795, TREEWORLD, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TREEWORLD,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-010	Malicious File Transfer - UNC5795, TREEWORLD, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TREEWORLD,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-011	Malicious File Transfer - UNC5795, TREEWORLD, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TREEWORLD,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-012	Malicious File Transfer - UNC5795, TREEWORLD, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TREEWORLD,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-013	Malicious File Transfer - UNC5795, TREEWORLD, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TREEWORLD,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-014	Malicious File Transfer - UNC5795, TREEWORLD, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TREEWORLD,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-015	Malicious File Transfer - UNC5866, SACREDDESK, Download, Variant #4	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
A108-016	Malicious File Transfer - UNC5866, SACREDGAME, Download, Variant #5	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
A108-017	Malicious File Transfer - UNC6085, BADMOVIE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADMOVIE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-018	Malicious File Transfer - UNC6085, CRUDEEXCLUDE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,CAMP.26.027,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CRUDEEXCLUDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-019	Malicious File Transfer - UNC6085, FOUDRE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,CAMP.26.027,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FOUDRE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-020	Malicious File Transfer - UNC6085, FOUDRE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FOUDRE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-021	Malicious File Transfer - UNC6085, FOUDRE, SFXRAR, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,CAMP.26.027,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FOUDRE,Malware:SFXRAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-022	Malicious File Transfer - UNC6085, FOUDRE, SFXRAR, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,CAMP.26.027,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FOUDRE,Malware:SFXRAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-023	Malicious File Transfer - UNC6085, HEAVYGRAM, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,CAMP.26.027,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HEAVYGRAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-024	Malicious File Transfer - UNC6085, LIGHTMASS, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,CAMP.26.027,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTMASS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-025	Malicious File Transfer - UNC6085, LIGHTMASS, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,CAMP.26.027,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LIGHTMASS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-026	Malicious File Transfer - UNC6085, PAPERDUST, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,CAMP.26.027,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PAPERDUST,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-027	Malicious File Transfer - UNC6085, PICKLEDIVE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,CAMP.26.027,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PICKLEDIVE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-028	Malicious File Transfer - UNC6085, SANDGLASS, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDGLASS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-029	Malicious File Transfer - UNC6085, SANDGLASS, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,CAMP.26.027,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDGLASS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-030	Malicious File Transfer - UNC6085, SFXRAR, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6085,CAMP.26.027,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SFXRAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-031	Malicious File Transfer - UNC6309, SPACEHAMMER, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6309,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SPACEHAMMER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-032	Malicious File Transfer - UNC6309, SPACEHAMMER, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6309,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SPACEHAMMER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-033	Malicious File Transfer - UNC6309, SPACEHAMMER, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6309,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SPACEHAMMER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-034	Malicious File Transfer - UNC6309, SPACEHAMMER, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6309,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SPACEHAMMER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-035	Malicious File Transfer - UNC6566, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6566,CAMP.25.079,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-036	Malicious File Transfer - UNC6566, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6566,CAMP.25.079,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-037	Malicious File Transfer - UNC6572, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6572,CAMP.26.019,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-038	Malicious File Transfer - UNC6572, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6572,CAMP.26.019,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-039	Malicious File Transfer - UNC6713, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6713,CAMP.26.017,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-040	Malicious File Transfer - UNC6713, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6713,CAMP.26.017,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-041	Malicious File Transfer - UNC6713, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6713,CAMP.26.017,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-042	Malicious File Transfer - UNC6713, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6713,CAMP.26.017,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-043	Phishing Email - Malicious Attachment, UNC5187, ENDDOT, Variant #1	ATT&CK:Initial Access,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:M1049,ATT&CK:M1054,ATT&CK:T1566.001,Actor:UNC5187,Control:Email,Malware:ENDDOT,NIST:CM-7,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-044	Phishing Email - Malicious Attachment, UNC5795, HOTAIR, Variant #1	ATT&CK:Initial Access,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:M1049,ATT&CK:M1054,ATT&CK:T1566.001,Actor:UNC5795,Control:Email,Malware:HOTAIR,NIST:CM-7,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-045	Phishing Email - Malicious Attachment, UNC6309, SPACEHAMMER, Variant #1	ATT&CK:Initial Access,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:M1049,ATT&CK:M1054,ATT&CK:T1566.001,Actor:UNC6309,Control:Email,Malware:SPACEHAMMER,NIST:CM-7,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-046	Phishing Email - Malicious Link, UNC6729, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC6729,CAMP.26.024,Control:Email,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-047	Phishing Email - Malicious Link, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Control:Email,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted

Host CLI Actions

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-943	Host CLI - Add Defender Exclusion Via Batch Script, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.001,CAMP.26.013,CWE:284,Control:Endpoint,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A107-944	Host CLI - APT34, ENDDOT, Defense Evasion Via Timestomp, Variant #1	ATT&CK:Defense Evasion,ATT&CK:T1070.006,Actor:APT34,Actor:UNC5187,Control:Endpoint,Malware:ENDDOT,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
A107-945	Host CLI - UNC5866, SPACEHAMMER, Simulate Overwriting User Files, Variant #1	ATT&CK:Impact,ATT&CK:M1053,ATT&CK:T1485,Actor:UNC5866,CAMP.26.021,Control:Endpoint,Impact:Availability,Malware:SPACEHAMMER,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A107-946	Host CLI - UNC6713, Add Windows Defender Exclusion, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.001,Actor:UNC6713,CAMP.26.017,CWE:284,Control:Endpoint,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted

Protected Theater Actions

VID	Name	Tags
A108-048	Protected Theater - Exfiltrate Data Via Encoded Powershell Command, Variant #1	ATT&CK:Execution,ATT&CK:M1026,ATT&CK:M1038,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1049,ATT&CK:T1059.001,CAMP.26.013,Control:Endpoint,NIST:CM-11,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-049	Protected Theater - SACREDDESK, Execute And Drop Component Dlls, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5866,CAMP.26.021,Control:Endpoint,Malware:SACREDDESK,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-050	Protected Theater - SACREDGAME, Execute And Connect To C2, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5866,CAMP.26.021,Control:Endpoint,Malware:SACREDGAME,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-051	Protected Theater - UNC5655, ERIESNAKE.GO, Executes And Connects To A C2 Domain, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5655,Control:Endpoint,Malware:ERIESNAKE.GO,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-052	Protected Theater - UNC5795, HOTAIR, Drops Masqueraded Crowdstrike Executable, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1038,ATT&CK:M1045,ATT&CK:T1036.005,Actor:UNC5795,Control:Endpoint,Malware:HOTAIR,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-053	Protected Theater - UNC5795, HOTAIR, Executes Installer To Drop Jperf.Exe, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5795,Control:Endpoint,Malware:HOTAIR,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-054	Protected Theater - UNC5795, HOTAIR, Installer Drops `Crowdstrike.Exe`, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1038,ATT&CK:M1045,ATT&CK:T1036.005,Actor:UNC5795,Control:Endpoint,Malware:HOTAIR,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-055	Protected Theater - UNC5795, HOTAIR, Ladesk Service Creation, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC5795,CWE:284,Control:Endpoint,Malware:HOTAIR,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-056	Protected Theater - UNC5795, HOTAIR, Run Key For Microsoft.Teams.Api.Exe, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC5795,Control:Endpoint,Malware:HOTAIR,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-057	Protected Theater - UNC5795, HOTAIR, Scheduled Task For Updater.Exe, Variant #1	ATT&CK:Execution,ATT&CK:M1018,ATT&CK:M1026,ATT&CK:M1028,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1053.005,Actor:UNC5795,Control:Endpoint,Malware:HOTAIR,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-058	Protected Theater - UNC5795, HOTAIR, To Drop A Secondary Payload, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5795,Control:Endpoint,Malware:HOTAIR,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-059	Protected Theater - UNC5795, Installer Dropping Masqueraded Payload, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1038,ATT&CK:M1045,ATT&CK:T1036.005,Actor:UNC5795,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-060	Protected Theater - UNC5795, 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:UNC5795,Control:Endpoint,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-061	Protected Theater - UNC5795, Persistence Via Startup Folder, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1060,ATT&CK:T1547.001,Actor:UNC5795,Control:Endpoint,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-062	Protected Theater - UNC5795, Scheduled Task 'Googleupdater', Variant #1	ATT&CK:Execution,ATT&CK:M1018,ATT&CK:M1026,ATT&CK:M1028,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1053.005,Actor:UNC5795,Control:Endpoint,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-063	Protected Theater - UNC5795, TREEWORLD, 4.Exe, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5795,Control:Endpoint,Malware:TREEWORLD,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-064	Protected Theater - UNC5795, TREEWORLD, Executes And Connects To C2, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5795,Control:Endpoint,Malware:TREEWORLD,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-065	Protected Theater - UNC5795, TREEWORLD, Executes Batch Script, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC5795,Control:Endpoint,Malware:TREEWORLD,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-066	Protected Theater - UNC5795, TREEWORLD, Executes Malicious Dll Via Rundll32, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1050,ATT&CK:T1218.011,Actor:UNC5795,CWE:114,Control:Endpoint,Malware:TREEWORLD,NIST:CM-11,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-067	Protected Theater - UNC5866, SACREDDESK, 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:UNC5866,CAMP.26.021,Control:Endpoint,Malware:SACREDDESK,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-068	Protected Theater - UNC5866, SACREDDESK, 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:UNC5866,CAMP.26.021,Control:Endpoint,Malware:SACREDDESK,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-069	Protected Theater - UNC6085, FOUDRE, SFXRAR, Dropper Execution, Variant #2	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6085,CAMP.26.027,Control:Endpoint,Malware:FOUDRE,Malware:SFXRAR,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A108-070	Protected Theater - UNC6085, FOUDRE, SFXRAR, Dropper, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6085,CAMP.26.027,Control:Endpoint,Malware:FOUDRE,Malware:SFXRAR,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A108-071	Protected Theater - UNC6085, FOUDRE, SFXRAR, Drops Conf6318.Dll, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6085,CAMP.26.027,Control:Endpoint,Malware:FOUDRE,Malware:SFXRAR,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-072	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,CAMP.26.027,Control:Endpoint,Malware:FOUDRE,Malware:SFXRAR,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-073	Protected Theater - UNC6309, SPACEHAMMER, Creates A Fake Google Updater Service For Persistence, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC6309,CAMP.26.021,CWE:284,Control:Endpoint,Malware:SPACEHAMMER,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-074	Protected Theater - UNC6309, SPACEHAMMER, Executes Dropper To Drop Secondary Payload, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6309,Control:Endpoint,Malware:SPACEHAMMER,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-075	Protected Theater - UNC6309, SPACEHAMMER, Executes Msi Installer, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6309,CAMP.26.021,Control:Endpoint,Malware:SPACEHAMMER,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-076	Protected Theater - UNC6309, SPACEHAMMER, Executes Powershell Script To Drop Wallpaper Image, Variant #1	ATT&CK:Execution,ATT&CK:M1026,ATT&CK:M1038,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1049,ATT&CK:T1059.001,Actor:UNC6309,Control:Endpoint,Malware:SPACEHAMMER,NIST:CM-11,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-077	Protected Theater - UNC6309, SPACEHAMMER, Install Msi Package, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1026,ATT&CK:M1042,ATT&CK:T1218.007,Actor:UNC6309,Control:Endpoint,Malware:SPACEHAMMER,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-078	Protected Theater - UNC6572, Connects To C2, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6572,CAMP.26.019,Control:Endpoint,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-079	Protected Theater - UNC6713, Directory Integrity Level Modification, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1026,ATT&CK:T1222.001,Actor:UNC6713,CAMP.26.017,Control:Endpoint,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-080	Protected Theater - UNC6713, Executes Malicious Installer To Drop Payload, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6713,CAMP.26.017,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A108-081	Protected Theater - UNC6713, 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:UNC6713,CAMP.26.017,Control:Endpoint,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-082	Protected Theater - UNC6713, 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:UNC6713,CAMP.26.017,Control:Endpoint,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-083	Protected Theater - UNC6713, To Drop Executable Payload, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6713,CAMP.26.017,Control:Endpoint,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

New Files

A total of 98 new files have been added to the File Library with this update. This includes 98 malicious files and 0 non-malicious files.

Malicious Files

File MD5	Tags
00a70b29400e984d4451e567f5e8e449	Group:Validation
013568279e0f9d8ff43754e94b756517	Group:Validation,Malware_Type:DOWNLOADER
013e5298cbb113614f01dfd55bce0d60	Malware_Type:DROPPER,Malware:HOTAIR,Group:Validation
033b2924742f39c20436fc4ac303c123	Group:Validation,Malware_Type:BACKDOOR,Malware:ERIESNAKE.GO
0373bc7b1b8978b4df6b28a0eb97513d	Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
042e089a0f39065e9fc9ca18eb1d3277	Malware_Type:BACKDOOR,Malware:ERIESNAKE.GO,Group:Validation
09e83162a6b0bae4b94f21bd6100e33f	Malware:HOTAIR,Group:Validation,Malware_Type:INSTALLER
09fc4024fb30e33bf2dae1bea162c2bb	Group:Validation,Malware:SNARESEND,Malware_Type:DATA_MINER
0bd5fce00fbc5a7aeebe228d9899e84c	Malware_Type:BACKDOOR,Malware:ERIESNAKE.GO,Group:Validation
0c76c41dfe6989ba042e27755e2b68f7	Group:Validation,Malware:SPACENOISE,Malware_Type:BACKDOOR
0cffbdc6b5fe21f2ee3fe3ebc8f6f521	Malware_Type:INSTALLER,Group:Validation,Malware:HOTAIR
13c580177b7f486becb5f9f959276c52	Group:Validation,Malware:REGALSPICE,Malware_Type:BACKDOOR
176dd88821bddd6554cb668b0c49cccd	Malware:CHISEL,Group:Validation,Malware_Type:DROPPER_MEMORY_ONLY
180319b2c001fa4fb9ae1c6fc8b5b205	Malware_Type:BACKDOOR,Malware:HEAVYGRAM,Group:Validation
1a650573eb02a9faf93e9c1853a42f08	Malware_Type:DROPPER,Group:Validation
23a9131b1d9f6178dcde0c7c0dc99fec	Group:Validation
23d88fa3367125c47c67fb8400116c44	Malware:ENDDOT,Malware_Type:BACKDOOR,Group:Validation
259ea606256b61c1937bc9060de13430	Malware_Type:INSTALLER,Group:Validation,Malware:HOTAIR
26543bc49ebd323977bb15f41a70c6c7	Group:Validation,Malware:PICKLEDIVE,Malware_Type:DATA_MINER
26892452f724581530c45287c8b7bc67	Group:Validation,Malware:CRUDEEXCLUDE,Malware_Type:UTILITY
279bb277d858c1df7cd2ad1bbe8122fe	Group:Validation
29fb764985406cca18a4f430bfb00c3d	Group:Validation
2bc1c670a5c179e58f6c33c7469b9d98	Malware:ENDDOT,Group:Validation,Malware_Type:BACKDOOR
2d873e91ac1a0423b186bd4fbf8e50d0	Malware_Type:BACKDOOR,Malware:GRIDTIDE,Group:Validation
31de3c2b0eaec947217460a284f6f503	Malware_Type:DROPPER,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
36d177ba6a6262d7af096d8b6fd99cda	Group:Validation,Malware_Type:DOWNLOADER,Malware:BADMOVIE
379627f30864b8e715f5f4b20f101ded	Group:Validation,Malware_Type:BACKDOOR,Malware:ERIESNAKE
3e0b495c23b629a8f953e5c156ebabc5	Group:Validation,Malware:HOTAIR,Malware_Type:INSTALLER
45111cf3b67de485c926b818de9f3055	Malware_Type:INSTALLER,Group:Validation
459d973200cda0b4f0999d795fab8773	Malware_Type:INSTALLER,Group:Validation,Malware:HOTAIR
4978057735693c3343a74e0cee36c756	Group:Validation,Malware_Type:BACKDOOR,Malware:ENDDOT
4abe7fdf638fdf54bfc035e20a209cf6	Group:Validation
4b4cb57bc4aa1ba60cf67a065ba55151	Group:Validation,Malware:NEATSNAKE,Malware_Type:BACKDOOR
54f58e7c679f82d3512ab00798d359e0	Group:Validation
55a7bfcbe2f409be6230eb964d04f1fc	Malware:TREEWORLD,Malware_Type:BACKDOOR,Group:Validation
5b6dea8221f2233e3ac6baa19c27468b	Malware:SPACEHAMMER,Group:Validation
5c3017993b0342cf6240b1c7b34fb8c1	Group:Validation,Malware:AEROSTAT,Malware_Type:BACKDOOR
5d445b549817b7b485502ebeeda4f741	Group:Validation,Malware_Type:DROPPER
64d7cab18a3510cdc25a424db0da55c6	Malware:TREEWORLD,Group:Validation,Malware_Type:BACKDOOR
66126dc088be2699fd55ae7eff5e6e15	Malware:SPAREPRIZE,Group:Validation,Malware_Type:BACKDOOR
68ced35000663f1643c70869bddd42c9	Malware_Type:BACKDOOR,Malware:REGALSPICE,Group:Validation
6914d930998108adfc93b7fe1aa3e64e	Malware_Type:BACKDOOR,Group:Validation
6f9fb128e9eb14cff6bb84495e1b4cac	Malware_Type:BACKDOOR,Malware:SACREDGAME,Group:Validation
70a9b537b9b7e1b410576d798e6c5043	Group:Validation,Malware_Type:BACKDOOR,Malware:TREEWORLD
776677256087a5a0f543a6b6317cadf8	Malware_Type:BACKDOOR,Group:Validation,Malware:SPACENOISE

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
78fdf5dbc9f56c66d53a7d94d3b058b4	Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
791e0e51765d56455cb9b50b9df9e7d5	Malware:HOPEDFOR,Malware_Type:DOWNLOADER,Group:Validation
7976e4872b197251041c5f62d729796d	Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
7a74cedbf42172852b66452de631e807	Malware:TREEWORLD,Malware_Type:BACKDOOR,Group:Validation
7e3d2006f5c9f0f3d0789b51f64d566a	Malware_Type:LAUNCHER,Group:Validation
7f17fa22feaced1a16d4d39c545cdb16	Malware_Type:BACKDOOR,Malware:TREEWORLD,Group:Validation
7f2a2a15823a66993b7c2b504a0ae00a	Group:Validation
809139c237c4062baecab43570060d67	Malware:TREEWORLD,Group:Validation,Malware_Type:BACKDOOR
8243af256a47090488b757e6afa2d8f5	Malware:HOTAIR,Group:Validation,Malware_Type:DROPPER
8660fe091b4b6c551a6c96062e1cbba9	Group:Validation
88feeda8cd26284911bc004e977c7466	Group:Validation,Malware:ERIESNAKE.GO,Malware_Type:BACKDOOR
8a062a2d0741b57fab9635920b17275b	Group:Validation,Malware:CHISEL,Malware_Type:DROPPER_MEMORY_ONLY
90087f08cf933a6c4d2d51b6e8046837	Group:Validation
90cd84f9c953b702592eff034bbc0df6	Group:Validation
91932a912d071422dc8b095ea723e95c	Group:Validation,Malware:ERIESNAKE.GO,Malware_Type:BACKDOOR
922b88f1d601e0ff313a14904868eef6	Group:Validation
945fde5bfb9f05115eae18409398bf8e	Malware:ERIESNAKE.GO,Malware_Type:BACKDOOR,Group:Validation
986d76931e070a92ad59c3de09695c60	Group:Validation,Malware:HOTAIR,Malware_Type:DOWNLOADER
99641caf6758b75e23ed4587c9751a68	Group:Validation
9d6e8d36e9cf3047b22032b0621de73e	Group:Validation
a1c7cd918a6abb7a11153c49732246a0	Malware:ERIESNAKE.GO,Malware_Type:BACKDOOR,Group:Validation
a453a4ae9cbb58d8fd420abe53aac192	Malware_Type:INSTALLER,Malware:HOTAIR,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
a7561eb023bb2c4025defcfe758d8ac2	Group:Validation
ad40ba0e7e3e09042634bd308117ed3e	Malware_Type:INSTALLER,Group:Validation,Malware:HOTAIR
b08a4a7233edc8c57a973b7295eb6ffd	Group:Validation
b19add5ccaa17a1308993e6f3f786b06	Group:Validation,Malware_Type:BACKDOOR,Malware:TREEWORLD
b40533e67e70b7ff7bb53d34a4b9170e	Group:Validation,Malware_Type:BACKDOOR,Malware:SPACENOISE
b48221c6cbd2bc8b02cc1be852803df1	Malware:HOTAIR,Group:Validation,Malware_Type:INSTALLER
b49ce8f38f0dcf4cde6880535285f7b9	Malware_Type:BACKDOOR,Malware:HOPEDFOR,Group:Validation
b4d1d2e7040e6ae96bf8dcd9fdc6786a	Malware_Type:DOWNLOADER,Malware:SANDGLASS,Group:Validation
b5ad76ef744401aa648f56a83e0db00c	Group:Validation
b817309621e43004b9f32c96d52dc2a0	Malware_Type:DROPPER,Group:Validation,Malware:SPAREPRIZE
b9ec9334d93809bb818d37c056e5433a	Malware:SPACEHAMMER,Group:Validation
caecb47e161c8789ba965e67c27cda55	Group:Validation
ccc59903bc32a45929db836ea3c65fbb	Group:Validation
ceae7b77297ad467fa320a9b9fb049f2	Malware_Type:BACKDOOR,Malware:SANDGLASS,Group:Validation
d12d089d43a066554f2f65becb6975de	Malware_Type:BACKDOOR,Malware:MAILDOT,Group:Validation
d4f77f6188c428db6a1e17a73e71a99d	Malware:MAILDOT,Group:Validation,Malware_Type:BACKDOOR
d5a48bd67c16bd19ddf07baceb9153e4	Group:Validation
d5ddf40ba2506c57d3087d032d733e08	Group:Validation
d8a868700563f702c1d2714e59ebe831	Malware_Type:BACKDOOR,Malware:ERIESNAKE.GO,Group:Validation
dce41d9d1da0084e7e44847b1b2b9fe0	Malware:HOTAIR,Malware_Type:DROPPER,Group:Validation
e0763eb3c36f532b486a383d9ed35afd	Malware_Type:DOWNLOADER,Malware:LIGHTMASS,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
e275b96af7936f0c61b254bc9eed954a	Malware_Type:BACKDOOR,Malware:ERIESNAKE.GO,Group:Validation
e671ede7c3c8064b1e3a30ba46d1130e	Group:Validation,Malware_Type:DOWNLOADER,Malware:HOTAIR
e7d52ef521b8cd0b405575c185d64033	Malware:ENDDOT,Malware_Type:DROPPER,Group:Validation
ec3f93637cbb85d78a27fe277b7ac382	Group:Validation
eed66fe72a8a8c2ea98209cd09a35b90	Malware_Type:BACKDOOR,Group:Validation,Malware:ERIESNAKE.GO
f143f5a8ab7a5e86cad84a7e1e5f5b83	Group:Validation,Malware_Type:DOWNLOADER,Malware:PAPERDUST
f1d8513e01584f82d9491423a3cc0841	Group:Validation,Malware:HOTAIR,Malware_Type:INSTALLER
f2461cb7f009e123848daa39e1841fd8	Malware:SPACEHAMMER,Group:Validation,Malware_Type:DISRUPTION_TOOL
f277bb4ebefb21498a9fb3f89b9a7f37	Group:Validation
fc1eb02d16f56e1da74c9e62a447e568	Malware:ERIESNAKE.GO,Group:Validation,Malware_Type:BACKDOOR

Updated Content

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

Supported Operating Systems (OS) and Platforms

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

Mandiant Security Validation Platform

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

Network Actions

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

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.