Mandiant

VHR20260923 - SEPTEMBER 23, 2026

The Mandiant Intelligence Validation Research Team (VRT) has published VHR20260923 - Content Expansion. This content pack requires Director version 4.12.1.0-0 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

- 105 Actions added
- 71 Files added

Release Highlights

- A new Action covering **Campaign 24-045** (https://advantage.mandiant.com/campaigns/CAMP.24.045), a campaign by financially motivated actor **UNC5142** (https://advantage.mandiant.com/actors/UNC5142) that compromises vulnerable WordPress websites using "EtherHiding" to deliver **CLEARSHORT** (https://advantage.mandiant.com/malware/CLEARSHORT).
- New Actions demonstrating **Campaign 26-013** (https://advantage.mandiant.com/campaigns/CAMP.26.013), an intrusion campaign by **UNC6692** (https://advantage.mandiant.com/actors/UNC6692) that employs social engineering to deploy a custom SNOW malware suite, including **SNOWBELT** (https://advantage.mandiant.com/malware/SNOWBELT), **SNOWGLAZE** (https://advantage.mandiant.com/malware/SNOWGLAZE), and **SNOWBASIN** (https://advantage.mandiant.com/malware/SNOWBASIN), for data exfiltration.
- New Actions demonstrating **Campaign 26-069** (https://advantage.mandiant.com/campaigns/CAMP.26.069), a Russian financially motivated actor **UNC6910** (https://advantage.mandiant.com/actors/UNC6910) initial access campaign leveraging ClickFix social engineering to deliver **NEONSLIDE** (https://advantage.mandiant.com/malware/NEONSLIDE) and **CURLYGATE** (https://advantage.mandiant.com/malware/CURLYGATE).
- New Actions demonstrating **Campaign 26-125** (https://advantage.mandiant.com/campaigns/CAMP.26.125), a campaign by **UNC7072** (https://advantage.mandiant.com/actors/UNC7072) deploying **CLOUDHAZE** (https://advantage.mandiant.com/malware/CLOUDHAZE) malware via fake software lures and executing discovery scripts.
- New Actions covering **Campaign 26-106** (https://advantage.mandiant.com/campaigns/CAMP.26.106), an **UNC7003** (https://advantage.mandiant.com/actors/UNC7003) campaign that compromises public sector systems via IIS exploitation and custom rootkits, including **SLATEVINE** (https://advantage.mandiant.com/malware/SLATEVINE) and **IRONBARK** (https://advantage.mandiant.com/malware/IRONBARK).
- New Actions demonstrating **Campaign 26-129** (https://advantage.mandiant.com/campaigns/CAMP.26.129), where **APT42** (https://advantage.mandiant.com/actors/APT42) deploys **TAMECAT** (https://advantage.mandiant.com/malware/TAMECAT) via malicious LNK lures targeting the nuclear sector.
- New Actions demonstrating **Campaign 26-132** (https://advantage.mandiant.com/campaigns/CAMP.26.132), a financially motivated campaign leveraging ClickFix web compromises for macOS credential theft and extortion, using tools like **CURL** (https://advantage.mandiant.com/malware/CURL).
- A new Action demonstrating **Campaign 26-117** (https://advantage.mandiant.com/campaigns/CAMP.26.117), a suspected China-based threat actor **UNC7040** (https://advantage.mandiant.com/actors/UNC7040) campaign targeting entities in Taiwan with webshell exploitation, Certutil downloads, and extensive host reconnaissance.
- New Actions demonstrating **Campaign 26-135** (https://advantage.mandiant.com/campaigns/CAMP.26.135), an actor of unknown motivations' campaign leveraging deceptive browser installers to deploy **COLDRAIN** (https://advantage.mandiant.com/malware/COLDRAIN) and **SLOWJOG** (https://advantage.mandiant.com/malware/SLOWJOG) to hijack sessions.
- New Actions demonstrating **Campaign 26-136** (https://advantage.mandiant.com/campaigns/CAMP.26.136), a campaign by **UNC7129** (https://advantage.mandiant.com/actors/UNC7129) leveraging ClickFix commands to deploy encrypted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

payloads via PowerShell, ultimately delivering **GREYMOON** (https://advantage.mandiant.com/malware/GREYMOON).

- New Actions covering **Campaign 26-137** (https://advantage.mandiant.com/campaigns/CAMP.26.137), an unknown threat actor campaign leveraging **GREYMOON** (https://advantage.mandiant.com/malware/GREYMOON) and social engineering to deploy PowerShell payloads.
- A new Action covering **FLUXWEAVE** (https://advantage.mandiant.com/malware/FLUXWEAVE), a downloader used by **UNC6527** (https://advantage.mandiant.com/actors/UNC6527) in **Campaign 25-076** (https://advantage.mandiant.com/campaigns/CAMP.25.076) that leverages fake file converter software.
- New Actions demonstrating **Campaign 26-133** (https://advantage.mandiant.com/campaigns/CAMP.26.133), an actor **APT44** (https://advantage.mandiant.com/actors/APT44) campaign conducting phishing with malicious links to deploy VBS loaders that deliver **FEEDUPDATE** (https://advantage.mandiant.com/malware/FEEDUPDATE).
- New Actions demonstrating **Campaign 26-017** (https://advantage.mandiant.com/campaigns/CAMP.26.017), a campaign by **UNC6713** (https://advantage.mandiant.com/actors/UNC6713) deploying **NEONSLIDE** (https://advantage.mandiant.com/malware/NEONSLIDE) via ClickFix lures with scheduled task persistence and Defender evasion.

New Actions

A total of 105 Actions have been added to the content baseline with this update. This includes 105 Network Actions. All Actions in this release are tagged using the MITRE ATT&CK v13 framework.

Network Actions

VID	Name	Tags
A109-306	Command and Control - APT44, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:APT44,CAMP.26.133,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-307	Command and Control - NEONSLIDE, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,GLOBAL.26.006,Malware:NEONSLIDE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-308	Command and Control - NEONSLIDE, Communication, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,GLOBAL.26.006,Malware:NEONSLIDE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-309	Command and Control - NEONSLIDE, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.006,Malware:NEONSLIDE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-310	Command and Control - UNC5142, PALEBEAM, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5142,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.009,Malware:PALEBEAM,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-311	Command and Control - UNC5142, PALEBEAM, Tasking, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5142,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.009,Malware:PALEBEAM,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-312	Command and Control - UNC6713, Check-In, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6713,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.009,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-313	Command and Control - UNC6713, Check-In, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6713,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.009,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-314	Command and Control - UNC6713, Check-In, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6713,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.009,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-315	Command and Control - UNC6713, Tasking, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6713,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.009,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-316	Command and Control - UNC6849, NEONSLIDE, Check-In, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6849,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.006,Malware:NEONSLIDE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-319	Command and Control - UNC7007, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-320	Command and Control - UNC7007, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-321	Command and Control - UNC7007, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7007,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
A109-322	Command and Control - UNC7007, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-323	Command and Control - UNC7007, Registration, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-324	Command and Control - UNC7007, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-325	Command and Control - UNC7007, Tasking, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-326	Command and Control - UNC7007, Tasking, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-327	Command and Control - UNC7007, Tasking, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-328	Command and Control - UNC7007, Tasking, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-329	Command and Control - UNC7007, VIDAR, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:VIDAR,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-330	Command and Control - UNC7007, VIDAR, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VIDAR,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-331	Command and Control - UNC7007, VIDAR, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VIDAR,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-332	Command and Control - UNC7007, VIDAR, Tasking, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VIDAR,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-333	Command and Control - UNC7017, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7017,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-334	Command and Control - UNC7072, CLOUDHAZE, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7072,CAMP.26.125,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:CLOUDHAZE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-335	Command and Control - UNC7072, CLOUDHAZE, Exfiltration, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7072,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CLOUDHAZE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-336	Command and Control - UNC7072, CLOUDHAZE, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7072,CAMP.26.125,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CLOUDHAZE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-337	Command and Control - UNC7072, CLOUDHAZE, Tasking, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7072,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:CLOUDHAZE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-338	Command and Control - UNC7095, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7095,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,GLOBAL.26.010,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-339	Command and Control - UNC7095, Tasking, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7095,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,GLOBAL.26.010,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-340	Command and Control - UNC7095, Tasking, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7095,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,GLOBAL.26.010,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-341	Command and Control - UNC7129, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC7129,CAMP.26.136,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-342	Malicious File Transfer - APT42, TAMECAT, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,CAMP.26.129,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TAMECAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-343	Malicious File Transfer - APT42, TAMECAT, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT42,CAMP.26.129,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TAMECAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-344	Malicious File Transfer - APT44, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT44,CAMP.26.133,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-345	Malicious File Transfer - APT44, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT44,CAMP.26.133,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-346	Malicious File Transfer - APT44, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT44,CAMP.26.133,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-347	Malicious File Transfer - APT44, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT44,CAMP.26.133,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-348	Malicious File Transfer - APT44, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT44,CAMP.26.133,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-349	Malicious File Transfer - APT44, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT44,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-350	Malicious File Transfer - APT44, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT44,CAMP.26.133,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
A109-351	Malicious File Transfer - APT44, FEEDUPDATE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT44,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FEEDUPDATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-352	Malicious File Transfer - APT44, FEEDUPDATE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT44,CAMP.26.133,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FEEDUPDATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-353	Malicious File Transfer - APT44, FEEDUPDATE, FEEDUPDATE.MEOW, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT44,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FEEDUPDATE,Malware:FEEDUPDATE.MEOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-354	Malicious File Transfer - CURLYGATE, Download, Variant #21	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.069,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-355	Malicious File Transfer - GODPOTATO, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.117,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GODPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-356	Malicious File Transfer - NEONSLIDE, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.069,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-357	Malicious File Transfer - NEONSLIDE, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-358	Malicious File Transfer - NEONSLIDE, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-359	Malicious File Transfer - NEONSLIDE, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-360	Malicious File Transfer - NEONSLIDE, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-361	Malicious File Transfer - NEONSLIDE, Download, Variant #15	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-362	Malicious File Transfer - NEONSLIDE, Download, Variant #16	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-363	Malicious File Transfer - NEONSLIDE, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-364	Malicious File Transfer - UNC5142, PALEBEAM, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5142,CAMP.24.045,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PALEBEAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-365	Malicious File Transfer - UNC5976, HEADRUSH, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5976,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HEADRUSH,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-366	Malicious File Transfer - UNC6004, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6004,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-367	Malicious File Transfer - UNC6266, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6266,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-368	Malicious File Transfer - UNC6266, FROSTVALE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6266,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FROSTVALE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-369	Malicious File Transfer - UNC6266, FROSTVALE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6266,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FROSTVALE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-370	Malicious File Transfer - UNC6266, FROSTVALE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6266,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FROSTVALE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-371	Malicious File Transfer - UNC6266, FROSTVALE, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6266,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FROSTVALE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-372	Malicious File Transfer - UNC6266, FROSTVALE, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6266,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FROSTVALE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-373	Malicious File Transfer - UNC6266, FROSTVALE, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6266,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FROSTVALE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-374	Malicious File Transfer - UNC6266, KRYOSTAT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6266,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:KRYOSTAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-375	Malicious File Transfer - UNC6527, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6527,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-376	Malicious File Transfer - UNC6527, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6527,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-377	Malicious File Transfer - UNC6527, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6527,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
A109-378	Malicious File Transfer - UNC6527, FLUXWEAVE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6527,CAMP.25.076,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FLUXWEAVE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-379	Malicious File Transfer - UNC6527, FLUXWEAVE, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6527,CAMP.25.076,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FLUXWEAVE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-380	Malicious File Transfer - UNC6692, SNOWBASIN, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6692,CAMP.26.013,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SNOWBASIN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-381	Malicious File Transfer - UNC6692, SNOWBELT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6692,CAMP.26.013,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SNOWBELT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-382	Malicious File Transfer - UNC6713, Download, Variant #5	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
A109-383	Malicious File Transfer - UNC6713, Download, Variant #6	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
A109-384	Malicious File Transfer - UNC6935, CURL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6935,CAMP.26.132,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-385	Malicious File Transfer - UNC6935, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6935,CAMP.26.132,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
A109-386	Malicious File Transfer - UNC6935, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6935,CAMP.26.132,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-387	Malicious File Transfer - UNC6971, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6971,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-388	Malicious File Transfer - UNC7003, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7003,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-389	Malicious File Transfer - UNC7003, SLATEVINE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7003,CAMP.26.106,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLATEVINE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-390	Malicious File Transfer - UNC7003, SLATEVINE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7003,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLATEVINE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-392	Malicious File Transfer - UNC7007, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-393	Malicious File Transfer - UNC7007, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-394	Malicious File Transfer - UNC7007, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-395	Malicious File Transfer - UNC7007, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-396	Malicious File Transfer - UNC7007, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7007,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
A109-397	Malicious File Transfer - UNC7007, VIDAR, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7007,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VIDAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-398	Malicious File Transfer - UNC7033, FACTSPIN, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7033,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FACTSPIN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-399	Malicious File Transfer - UNC7033, PEERNOTE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7033,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PEERNOTE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-400	Malicious File Transfer - UNC7040, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7040,CAMP.26.117,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-401	Malicious File Transfer - UNC7060, COLDRAIN, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7060,CAMP.26.135,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:COLDRAIN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-402	Malicious File Transfer - UNC7060, COLDRAIN, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7060,CAMP.26.135,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:COLDRAIN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-403	Malicious File Transfer - UNC7060, SLOWJOG, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7060,CAMP.26.135,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLOWJOG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-404	Malicious File Transfer - UNC7095, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7095,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-405	Malicious File Transfer - UNC7095, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7095,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
A109-406	Malicious File Transfer - UNC7095, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7095,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-407	Malicious File Transfer - UNC7095, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7095,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-408	Malicious File Transfer - UNC7098, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7098,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-409	Malicious File Transfer - UNC7104, GREYMOON, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7104,CAMP.26.137,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYMOON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-410	Malicious File Transfer - UNC7104, GREYMOON, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7104,CAMP.26.137,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYMOON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-411	Malicious File Transfer - UNC7129, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7129,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-412	Malicious File Transfer - UNC7129, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7129,CAMP.26.136,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-413	Phishing Email - Malicious Attachment, UNC7104, GREYMOON, 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:UNC7104,CAMP.26.137,Control:Email,Malware:GREYMOON,NIST:CM-7,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted

New Files

A total of 71 new files have been added to the File Library with this update.This includes 71 malicious files.

Malicious Files

File MD5	Tags

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
015eaa36068e6b96eda901b250c7d2c9	Malware:NEONSLIDE,Malware_Type:DOWNLOADER,Group:Validation
06ca270080e2512d4a0b25a3b795555b	Group:Validation
0997582d828ef8460cda247a3915d18e	Group:Validation
108d36e1cc6f02da74e26d2052be7350	Malware:SLOWJOG,Malware_Type:INSTALLER,Group:Validation
10b4d54865310c0ce728c427a568a441	Malware:NEONSLIDE,Malware_Type:DOWNLOADER,Group:Validation
1a789fa1daa8e27b59174b0e9d0cac07	Group:Validation,Malware_Type:DRIVER
1b57025e1dd1bc4ff7b52a6b6a1df421	Group:Validation
1e672aae870776de0615676dc04decec	Malware:GREYMOON,Malware_Type:DOWNLOADER,Group:Validation
1fdb1dd742674d3939f636c3fc4b761f	Malware:GODPOTATO,Malware_Type:DRIVER,Group:Validation
2145d105663f93dc64e9b1c694ad84b4	Malware:FEEDUPDATE,Malware_Type:DOWNLOADER,Group:Validation
2396bd903fa1db27602a8d9673fa6d00	Malware_Type:BACKDOOR,Group:Validation
240e458e093924d7871092ffc5f62908	Malware:COLDRAIN,Malware_Type:INSTALLER,Group:Validation
286a930a6c3a0a24062ad3405d0002e0	Malware:FLUXWEAVE,Malware_Type:DOWNLOADER,Group:Validation
29e60ed43cb4814587a54c9990b4f2a5	Group:Validation
2c4487930d431aa31cc6dbd6a82e5f4e	Group:Validation
3153f113ca4ca05fd95ae16f26c0825e	Malware:SLATEVINE,Malware_Type:WEBSHELL,Group:Validation
325fee1cd327e51b1bfcebc4b5e61f9e	Group:Validation
328b37e46df07ac8b09dd5c8e9361612	Malware_Type:DRIVER,Group:Validation
3d6ea8576f78e16cb20735c9fc305bde	Malware:COLDRAIN,Malware_Type:DOWNLOADER,Group:Validation
3d9fca5dae96d533b1e762f28991b73c	Malware:FROSTVALE,Malware_Type:BACKDOOR,Group:Validation
3ecf248ffc792401c80f6f63d0d1829b	Group:Validation,Malware_Type:BACKDOOR
41f8268db8e61730314912530f6ebd60	Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
4747657ef7c0c74d7d3e756305e8e0a6	Malware:FROSTVALE,Malware_Type:BACKDOOR,Group:Validation
47ba02fcb0589a99ef3207840eb3b03a	Malware:NEONSLIDE,Malware_Type:DOWNLOADER,Group:Validation
4929f39ac40115efa58f7d25e63079d1	Group:Validation
4e58ae2ddbc2a6cba41fc70aa6b5c1e3	Malware:PALEBEAM,Malware_Type:DOWNLOADER,Group:Validation
4e7dded4ae4f93cdb039e48125ce5f0f	Malware:KRYOSTAT,Malware_Type:BACKDOOR,Group:Validation
5166033d818a1d9ba117fe43eabb2a35	Malware_Type:DROPPER,Malware:HEADRUSH,Group:Validation
51e0149f93935807996dc12f7cde37c0	Group:Validation
54f9c8b515a4182a735c95e0552bdc61	Malware_Type:UTILITY,Group:Validation
55d757b88f6e1846de4dae5785fbaa9b	Group:Validation
5da610ebcc9121d70f7b13e9d6b9a316	Malware:FROSTVALE,Malware_Type:BACKDOOR,Group:Validation
62b63f5f850b21465d3048ca84c9bf08	Group:Validation
63b70d8d33b511d956a2d215af07b5f9	Malware:NEONSLIDE,Malware_Type:DOWNLOADER,Group:Validation
65a14c42358f8da7a450089141bdc690	Malware:FEEDUPDATE,Malware_Type:DOWNLOADER,Group:Validation
78d57ba368597552af43c59ac390fc83	Malware:SNOWBELT,Malware_Type:BACKDOOR,Group:Validation
7bc851f8693ca8cb0f211d7e0fcd8827	Malware_Type:UTILITY,Group:Validation
8448e1c20d469eae44d4741bff90a010	Malware:NEONSLIDE,Malware_Type:DOWNLOADER,Group:Validation
85c07875f22388bd01cfadaf63284ab6	Malware_Type:DOWNLOADER,Group:Validation
85e2eb00efa63e501bbd9abc8cedd54e	Malware:FLUXWEAVE,Malware_Type:DOWNLOADER,Group:Validation
8dee18519b2fc76ed2cbe794118fbcb2	Malware:GREYMOON,Malware_Type:DOWNLOADER,Group:Validation
8ffbb0a21331410035931c5256ed019e	Malware:SLATEVINE,Malware_Type:WEBSHELL,Group:Validation
9003e6d34de2cd593132de7ecad4e888	Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
9a0f66df80e178ec2695aeeed7d54365	Malware:FACTSPIN,Malware_Type:BACKDOOR,Group:Validation
a1a421c178a5a8117da84197c9377acb	Group:Validation
a426262a08e9eeb3860feb604a1851bd	Malware_Type:LAUNCHER,Group:Validation
b0c7ed0c65a258c4b86e58f741995a86	Malware:NEONSLIDE,Malware_Type:DOWNLOADER,Group:Validation
b304986e947fe26a40e454426d90ef50	Group:Validation
b5e17102fbf39157f54a5416edb0dd0a	Group:Validation
b6a79851dcebb8e3b644581fad115be3	Malware:FEEDUPDATE.MEOW,Malware_Type:DOWNLOADER,Group:Validation
bec6ff96721285e7c61fbbed3e231aea	Malware_Type:DOWNLOADER,Group:Validation
c06f9dccc38ed250b2e013d40d5d8eb6	Group:Validation
c27ea04c17c9185ce83287f03f41360d	Malware:TAMECAT,Malware_Type:BACKDOOR,Group:Validation
c5850b3ebae3790941614429a7d9322b	Group:Validation
c7184d7a652618764fa6e2f2c0c33819	Group:Validation,Malware_Type:DOWNLOADER,Malware:CURLYGATE
cb4bba75beee8569e540f3369a96c657	Malware:TAMECAT,Malware_Type:BACKDOOR,Group:Validation
cc99429210a9c686f52b103cfb8af63e	Malware:PEERNOTE,Malware_Type:DROPPER,Group:Validation
ce3dbe65a25259e2ad6ed098f0276bee	Malware:FROSTVALE,Malware_Type:BACKDOOR,Group:Validation
cf7f05d4a8ce5cb83a347fe18ff67fd8	Group:Validation
d19aaafae14918c7fd866a8ad37f1b20	Group:Validation
d2a078cd9a992138d11e52f8c8b113b5	Malware:FROSTVALE,Malware_Type:BACKDOOR,Group:Validation
d5ee49ae728a699c89224d5f860ec83d	Malware:VIDAR,Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
dc95e13f49f668c9d952b21d9c0d8e99	Group:Validation
e05a8c4f5520393645eb6ee2f9896377	Group:Validation,Malware:GREYMOON,Malware_Type:DOWNLOADER

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
e0eb4dd662221538fe168b0747b79017	Malware:NEONSLIDE,Malware_Type:DOWNLOADER,Group:Validation
e5369da7563a7898f51033a2e9ce6d40	Group:Validation
e78087369c4c914df716891a9c125857	Malware:CURL,Malware_Type:DOWNLOADER,Group:Validation
e8b749d0ca0a2564a14ee0f918cbb103	Malware:NEONSLIDE,Malware_Type:DOWNLOADER,Group:Validation
ea3590ecf7f83f8cd5e2773f11ac1131	Malware:SNOWBASIN,Malware_Type:BACKDOOR,Group:Validation
f59a95615f9aef4d181ee83165879382	Malware_Type:DOWNLOADER,Group:Validation
f619c46b68b06412b476c841bb09cb8d	Malware:FROSTVALE,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 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	4.11.1.0-95
Actor	4.11.1.0-95

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.