Mandiant

VHR20260722 - JULY 22, 2026

The Mandiant Intelligence Validation Research Team (VRT) has published VHR20260722 - 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

- 109 Actions added
- 88 Files added

Release Highlights

- A new Action covering **Campaign 26-069** (https://advantage.mandiant.com/campaigns/CAMP.26.069), an initial access campaign by actor **UNC6910** (https://advantage.mandiant.com/actors/UNC6910) leveraging social engineering lures and delivering **CURLYGATE** (https://advantage.mandiant.com/malware/CURLYGATE), **CURLYFENCE** (https://advantage.mandiant.com/malware/CURLYFENCE), and **NEONSLIDE** (https://advantage.mandiant.com/malware/NEONSLIDE) malware.
- A new Action covering **Campaign 26-014** (https://advantage.mandiant.com/campaigns/CAMP.26.014), involving North Korea-nexus threat actor **UNC5342** (https://advantage.mandiant.com/actors/UNC5342) deploying Python backdoors such as **JADESNOW** (https://advantage.mandiant.com/malware/JADESNOW) and **INVISIBLEFERRET.JAVASCRIPT** (https://advantage.mandiant.com/malware/INVISIBLEFERRET.JAVASCRIPT) to target GitHub repositories for unauthorized code modification.
- New Actions demonstrating **Campaign 26-068** (https://advantage.mandiant.com/campaigns/CAMP.26.068), a campaign by **UNC6468** (https://advantage.mandiant.com/actors/UNC6468) using recipe-themed executables to deliver **PINESAP** (https://advantage.mandiant.com/malware/PINESAP) and establish initial access.
- New Actions demonstrating **Campaign 26-072** (https://advantage.mandiant.com/campaigns/CAMP.26.072), a China-nexus financial gain campaign by **UNC6727** (https://advantage.mandiant.com/actors/UNC6727) leveraging trojanized VPN installers to deploy **SUNBRICKED** (https://advantage.mandiant.com/malware/SUNBRICKED) malware.
- A new Action covering **Campaign 26-087** (https://advantage.mandiant.com/campaigns/CAMP.26.087), a campaign leveraging financial-themed phishing and malicious VBS scripts to target US government entities and deploy **BADWRAP** (https://advantage.mandiant.com/malware/BADWRAP).
- New Actions demonstrating **Campaign 26-085** (https://advantage.mandiant.com/campaigns/CAMP.26.085), a North Korean threat actor campaign targeting developer environments and CI/CD pipelines to facilitate DeFi supply chain compromises, leveraging **GATEKEEPER** (https://advantage.mandiant.com/malware/GATEKEEPER) and **SOMBERMEME** (https://advantage.mandiant.com/malware/SOMBERMEME) malware.
- A new Action covering **Campaign 26-080** (https://advantage.mandiant.com/campaigns/CAMP.26.080), a financially motivated actor campaign deploying malicious LNK payloads via fake browser updates to establish persistence.
- New Actions detailing **Campaign 24-061** (https://advantage.mandiant.com/campaigns/CAMP.24.061), where financially motivated threat actor **UNC5518** (https://advantage.mandiant.com/actors/UNC5518) distributes **FAKETREFF** (https://advantage.mandiant.com/malware/FAKETREFF) leading to other payloads including **QUICKBIND** (https://advantage.mandiant.com/malware/QUICKBIND), NETSUPPORT, **BANANACOOKIE** (https://advantage.mandiant.com/malware/BANANACOOKIE), CLEANBOOST, **CORNFLAKE** (https://advantage.mandiant.com/malware/CORNFLAKE), **DARKGATE** (https://advantage.mandiant.com/malware/DARKGATE), and **VOLTMARKER** (https://advantage.mandiant.com/malware/VOLTMARKER) via fake browser updates.
- New Actions demonstrating **Campaign 26-083** (https://advantage.mandiant.com/campaigns/CAMP.26.083), a suspected East Asia-nexus actor utilizing masqueraded dual-use tools and VBScript to download secondary payloads from cloud infrastructure.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

New Actions

A total of 109 Actions have been added to the content baseline with this update. This includes 109 Network Actions. All Actions in this release are tagged using the MITRE ATT&CK v13 framework.

Network Actions

VID	Name	Tags
A109-128	Command and Control - UNC1151, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-129	Command and Control - UNC1151, Check-In, Variant #2	ATT&CK:Command and Control,ATT&CK:Discovery,ATT&CK:M1031,ATT&CK:T1016.001,ATT&CK:T1071.001,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-130	Command and Control - UNC1151, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1031,ATT&CK:M1038,ATT&CK:M1045,ATT&CK:T1036.005,ATT&CK:T1071.001,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-131	Command and Control - UNC1151, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1071.001,ATT&CK:T1567,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-132	Command and Control - UNC5342, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:Discovery,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,ATT&CK:T1082,Actor:UNC5342,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-133	Command and Control - UNC5342, INVISIBLEFERRET, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:Discovery,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1614,Actor:UNC5342,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:INVISIBLEFERRET,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-134	Command and Control - UNC5342, JADESNOW, 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:UNC5342,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:JADESNOW,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-136	Command and Control - UNC5342, JADESNOW, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5342,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:JADESNOW,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-137	Command and Control - UNC5342, JADESNOW, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,Actor:UNC5342,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:JADESNOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-138	Command and Control - UNC5342, JADESNOW, Tasking, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,Actor:UNC5342,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:JADESNOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-139	Command and Control - UNC5518, PLYCHIP, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:Defense Evasion,ATT&CK:Execution,ATT&CK:M1026,ATT&CK:M1031,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1049,ATT&CK:T1027,ATT&CK:T1059.001,ATT&CK:T1071.001,ATT&CK:T1105,Actor:UNC5518,CWE:173,CWE:20,CWE:697,CWE:74,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PLYCHIP,NIST:AC-4,NIST:CM-11,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-140	Command and Control - UNC5518, PLYCHIP, Tasking, Variant #2	ATT&CK:Command and Control,ATT&CK:Discovery,ATT&CK:Execution,ATT&CK:M1026,ATT&CK:M1031,ATT&CK:M1038,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1049,ATT&CK:T1059.001,ATT&CK:T1071.001,ATT&CK:T1082,ATT&CK:T1105,Actor:UNC5518,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PLYCHIP,NIST:CM-11,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-141	Command and Control - UNC5774, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:M1037,ATT&CK:T1071.001,ATT&CK:T1572,Actor:UNC5774,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-142	Command and Control - UNC5774, Check-In, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5774,Control:IDS/IPS,Control:NGFW,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-143	Command and Control - UNC5774, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102.002,Actor:UNC5774,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-144	Command and Control - UNC5774, CORNFLAKE.V3, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:M1037,ATT&CK:T1071.001,ATT&CK:T1572,Actor:UNC5774,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:CORNFLAKE.V3,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-145	Command and Control - UNC5774, CORNFLAKE.V3, Check-In, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5774,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CORNFLAKE.V3,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-146	Command and Control - UNC5774, CORNFLAKE.V3, Check-In, Variant #3	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102.002,Actor:UNC5774,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CORNFLAKE.V3,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-147	Command and Control - UNC5774, CORNFLAKE.V3, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5774,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CORNFLAKE.V3,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-148	Command and Control - UNC6468, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6468,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-149	Malicious File Transfer - PRINTSPOOFER, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.093,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PRINTSPOOFER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-150	Malicious File Transfer - UNC1151, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-151	Malicious File Transfer - UNC1151, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,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
A109-152	Malicious File Transfer - UNC1151, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-153	Malicious File Transfer - UNC1151, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-154	Malicious File Transfer - UNC1151, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-155	Malicious File Transfer - UNC1151, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-156	Malicious File Transfer - UNC1151, Download, Variant #15	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-157	Malicious File Transfer - UNC1151, Download, Variant #16	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-158	Malicious File Transfer - UNC1151, Download, Variant #17	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-159	Malicious File Transfer - UNC1151, Download, Variant #18	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-160	Malicious File Transfer - UNC1151, Download, Variant #19	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-161	Malicious File Transfer - UNC1151, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,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
A109-162	Malicious File Transfer - UNC1151, Download, Variant #20	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-163	Malicious File Transfer - UNC1151, Download, Variant #21	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-164	Malicious File Transfer - UNC1151, Download, Variant #22	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-165	Malicious File Transfer - UNC1151, Download, Variant #23	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-166	Malicious File Transfer - UNC1151, Download, Variant #24	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-167	Malicious File Transfer - UNC1151, Download, Variant #25	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-168	Malicious File Transfer - UNC1151, Download, Variant #26	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-169	Malicious File Transfer - UNC1151, Download, Variant #27	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-170	Malicious File Transfer - UNC1151, Download, Variant #28	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-171	Malicious File Transfer - UNC1151, Download, Variant #29	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,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
A109-172	Malicious File Transfer - UNC1151, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-173	Malicious File Transfer - UNC1151, Download, Variant #30	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-174	Malicious File Transfer - UNC1151, Download, Variant #31	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-175	Malicious File Transfer - UNC1151, Download, Variant #32	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-176	Malicious File Transfer - UNC1151, Download, Variant #33	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-177	Malicious File Transfer - UNC1151, Download, Variant #34	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-178	Malicious File Transfer - UNC1151, Download, Variant #35	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-179	Malicious File Transfer - UNC1151, Download, Variant #36	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-180	Malicious File Transfer - UNC1151, Download, Variant #37	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-181	Malicious File Transfer - UNC1151, Download, Variant #38	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,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
A109-182	Malicious File Transfer - UNC1151, Download, Variant #39	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-183	Malicious File Transfer - UNC1151, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-184	Malicious File Transfer - UNC1151, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-185	Malicious File Transfer - UNC1151, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-186	Malicious File Transfer - UNC1151, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-187	Malicious File Transfer - UNC1151, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-188	Malicious File Transfer - UNC1151, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-189	Malicious File Transfer - UNC1151, OYSTERFRESH, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1151,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:OYSTERFRESH,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-190	Malicious File Transfer - UNC5342, JADESNOW, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5342,CAMP.26.014,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:JADESNOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-191	Malicious File Transfer - UNC5518, PLYCHIP, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5518,CAMP.24.061,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PLYCHIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-192	Malicious File Transfer - UNC5774, CORNFLAKE, CORNFLAKE.V3, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5774,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CORNFLAKE,Malware:CORNFLAKE.V3,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-193	Malicious File Transfer - UNC5774, CORNFLAKE, CORNFLAKE.V3, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5774,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CORNFLAKE,Malware:CORNFLAKE.V3,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-194	Malicious File Transfer - UNC5774, CORNFLAKE, CORNFLAKE.V3, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5774,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CORNFLAKE,Malware:CORNFLAKE.V3,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-195	Malicious File Transfer - UNC5774, CORNFLAKE, CORNFLAKE.V3, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5774,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CORNFLAKE,Malware:CORNFLAKE.V3,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-196	Malicious File Transfer - UNC5774, CORNFLAKE, CORNFLAKE.V3, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5774,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CORNFLAKE,Malware:CORNFLAKE.V3,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-197	Malicious File Transfer - UNC5774, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5774,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-198	Malicious File Transfer - UNC5774, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5774,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-199	Malicious File Transfer - UNC6021, ADAPTAGENT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6021,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ADAPTAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-200	Malicious File Transfer - UNC6468, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6468,CAMP.26.068,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
A109-201	Malicious File Transfer - UNC6468, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6468,CAMP.26.068,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-202	Malicious File Transfer - UNC6468, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6468,CAMP.26.068,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-203	Malicious File Transfer - UNC6468, PINESAP, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6468,CAMP.26.068,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PINESAP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-204	Malicious File Transfer - UNC6468, PINESAP, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6468,CAMP.26.068,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PINESAP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-205	Malicious File Transfer - UNC6468, PINESAP, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6468,CAMP.26.068,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PINESAP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-206	Malicious File Transfer - UNC6468, PINESAP, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6468,CAMP.26.068,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PINESAP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-207	Malicious File Transfer - UNC6468, PINESAP, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6468,CAMP.26.068,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PINESAP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-208	Malicious File Transfer - UNC6468, PINESAP, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6468,CAMP.26.068,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PINESAP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-209	Malicious File Transfer - UNC6468, PINESAP, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6468,CAMP.26.068,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PINESAP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-210	Malicious File Transfer - UNC6468, PINESAP, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6468,CAMP.26.068,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PINESAP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-211	Malicious File Transfer - UNC6468, PINESAP, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6468,CAMP.26.068,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PINESAP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-212	Malicious File Transfer - UNC6468, PINESAP, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6468,CAMP.26.068,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PINESAP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-213	Malicious File Transfer - UNC6468, PINESAP, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6468,CAMP.26.068,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PINESAP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-214	Malicious File Transfer - UNC6557, LOGMEIN, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6557,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LOGMEIN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-215	Malicious File Transfer - UNC6557, LOGMEIN, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6557,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LOGMEIN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-216	Malicious File Transfer - UNC6557, LOGMEIN, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6557,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LOGMEIN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-217	Malicious File Transfer - UNC6557, SCREENCONNECT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6557,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SCREENCONNECT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-218	Malicious File Transfer - UNC6727, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6727,CAMP.26.072,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-219	Malicious File Transfer - UNC6727, SUNBRICKED, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6727,CAMP.26.072,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SUNBRICKED,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-220	Malicious File Transfer - UNC6727, SUNBRICKED, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6727,CAMP.26.072,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SUNBRICKED,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-221	Malicious File Transfer - UNC6727, SUNBRICKED, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6727,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SUNBRICKED,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-222	Malicious File Transfer - UNC6727, SUNBRICKED, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6727,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SUNBRICKED,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-223	Malicious File Transfer - UNC6727, SUNBRICKED, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6727,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SUNBRICKED,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-224	Malicious File Transfer - UNC6727, SUNBRICKED, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6727,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SUNBRICKED,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-225	Malicious File Transfer - UNC6727, SUNBRICKED, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6727,CAMP.26.072,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SUNBRICKED,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-226	Malicious File Transfer - UNC6836, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6836,CAMP.26.085,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-227	Malicious File Transfer - UNC6836, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6836,CAMP.26.085,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-228	Malicious File Transfer - UNC6836, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6836,CAMP.26.085,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-229	Malicious File Transfer - UNC6836, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6836,CAMP.26.085,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-230	Malicious File Transfer - UNC6884, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6884,CAMP.26.069,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-231	Malicious File Transfer - UNC6923, OAKSHADE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6923,CAMP.26.080,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:OAKSHADE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-232	Malicious File Transfer - UNC6932, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6932,CAMP.26.083,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
A109-233	Malicious File Transfer - UNC6932, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6932,CAMP.26.083,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-234	Malicious File Transfer - UNC6932, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6932,CAMP.26.083,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-235	Malicious File Transfer - UNC6949, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6949,CAMP.26.087,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-236	Malicious File Transfer - UNC6984, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6984,CAMP.26.093,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-237	Phishing Email - Malicious Attachment, UNC6557, LOGMEIN, 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:UNC6557,Control:Email,Malware:LOGMEIN,NIST:CM-7,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted

New Files

A total of 88 new files have been added to the File Library with this update. This includes 88 malicious files.

Malicious Files

File MD5	Tags
014a542fd29819be7e66a72e6cadd877	Malware_Type:BACKDOOR,Malware:ADAPTAGENT,Group:Validation
09026ed818becb4fd2a7b38bacd9446a	Group:Validation
0a3a9221e91bb978f79cfc1d55deadff	Group:Validation
0b193e7c0033fb5b62b62046390447de	Malware_Type:DOWNLOADER,Malware:JADESNOW,Group:Validation
102b83d4c803938a67fdcc7d34d5063f	Group:Validation
11590720540e152070274c2053da5c45	Group:Validation
1683716f26b4f37be8c7b776f379eb7d	Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
18037141794168b4e77380d48cdf600b	Group:Validation
180e3d5a7bba737c402c9a1b86bfce2a	Malware_Type:DOWNLOADER,Malware:PINESAP,Group:Validation
185180f522d34105bd457e6893747ff2	Group:Validation
1d52d8d1fa23de5bea23e49a97a55af8	Group:Validation
2002c7268ac90ae34012ac060f030377	Group:Validation
206b1e687bb06af446d9c67ad5dd391e	Group:Validation
20ecfa351609ade2bcc0f4ada30a532f	Malware:OYSTERFRESH,Malware_Type:DOWNLOADER,Group:Validation
29350715dc6e6c80d9ff9522826ff7d6	Group:Validation
32211379c44810a6bdf9672c4aa0e850	Group:Validation
36aebf555fc1a700cb934596de4eb656	Malware:CORNFLAKE.V3,Malware_Type:BACKDOOR,Group:Validation
3d96f407857914c19b2cc48c9d54238e	Malware_Type:LAUNCHER,Group:Validation
3e506529f1008d7a1ff20e488baf32f0	Malware_Type:DOWNLOADER,Malware:OAKSHADE,Group:Validation
425dbed05e53394a719c6e0986a9ce87	Malware_Type:DOWNLOADER,Group:Validation
439d2f4d252aa3d691570a30371c35fc	Malware_Type:LAUNCHER,Group:Validation
4679d06df620d39c1d7e47e8f3619855	Group:Validation
48c1066946723823bbada44097acbac6	Group:Validation
4a154ba923103ab96dc5155ab2c93953	Group:Validation
4a3f99e5d08bbec0f4d657672e1ab7b3	Malware_Type:DOWNLOADER,Malware:PINESAP,Group:Validation
4cce2030e5baf9feecb7f77342e07f84	Group:Validation
4fd6063141ef6edfeb23fdd8a1f97d2e	Group:Validation
562e9a8f70196717cd0a6e5c6b2337ea	Group:Validation
57fc13bd3dc8a2429cf80876adf51b5d	Malware:CORNFLAKE.V3,Malware:CORNFLAKE,Malware_Type:BACKDOOR,Group:Validation
5b1217ccc6fd336a1465b7ce6c395c39	Group:Validation
5fa825564b4ede126005a88ba9efbb54	Group:Validation
621274ab6a043f43c8b22aae619a1543	Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
6458265f48b9fb7f02ab3d0bfd335562	Malware:SUNBRICKED,Malware_Type:LAUNCHER,Group:Validation
6872e762ad08e54a7158359ff92e61dd	Malware_Type:INSTALLER,Malware:SUNBRICKED,Group:Validation
69853c843688d939affeb88ca2bfab13	Malware:CORNFLAKE.V3,Group:Validation,Malware_Type:BACKDOOR
70716ab620851190f9dc0e944310a84e	Group:Validation
72e594ead2413c093ef5b538f6d453aa	Group:Validation
73b08953b24ba872a0917c25c87b2513	Group:Validation
80808772980fe246bc91cf170b8f76cb	Group:Validation
82ac42fbb88742c06f410397186b2d76	Malware:LOGMEIN,Group:Validation
83c87034c11439c7350f92096d15c91b	Group:Validation
854d94c41b291f5ac024e45e02c66ba6	Group:Validation
86af5457faadcac97224bb33b8c0a871	Group:Validation
8d3754109b13508cea053a73b45a43d4	Malware_Type:DOWNLOADER,Malware:PINESAP,Group:Validation
8f6cec6f5436eb0fe79a1f26a1c663d4	Malware_Type:DOWNLOADER,Malware:SUNBRICKED,Group:Validation
968dc6deae730509257536d06c5425a5	Malware_Type:WEBSHELL,Group:Validation
973c9e55811bf4940a874d3b6e6e2e0c	Malware:PINESAP,Malware_Type:DOWNLOADER,Group:Validation
9801f62c97e5b328070158a8f7337747	Group:Validation
9905e21c43a4bcdb702281f078ef4a4f	Group:Validation
9d283f04f8762f0184b34bc330417d56	Group:Validation
9f1950591d1f40fd24c335a2fe56cb03	Malware:CORNFLAKE.V3,Malware_Type:BACKDOOR,Group:Validation
ab1a67562a8c19aae22ad3db049d4b89	Group:Validation
ae3ed27ef8f3ff2a649b3e0ed6b4ad47	Group:Validation
afbf2e669d51f0a564dd0d8225bda76a	Malware:SCREENCONNECT,Group:Validation
b0f785a5ce2e376545a726b3b38f51cc	Group:Validation
b3ca5cfd100089d13efcec71624290db	Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
b85d84805e51cfce459c760e6c37d50d	Group:Validation
ba34e438b07b5ae2f97403a2b7dd198c	Malware:PINESAP,Group:Validation,Malware_Type:DOWNLOADER
ba87e8afdeee0f74b0ddb6f32b5e0c56	Malware:PINESAP,Malware_Type:DOWNLOADER,Group:Validation
bac348b984420b9b04cba399442ff8f1	Malware:PINESAP,Malware_Type:DOWNLOADER,Group:Validation
c434461f917fcdb721c88fe6528b2357	Group:Validation
c4edf28177e72d1bfc482cf4d05a156b	Malware_Type:DOWNLOADER,Malware:SUNBRICKED,Group:Validation
ce441b0eafb9709382ddd5c91c47b337	Group:Validation
ce5d94ca2a066e831f8fd8f995f29314	Group:Validation
ce629bdbf4af58f6057efd24a5cece59	Group:Validation
d06c8c28654ec6fba03f8ee1f76b8641	Malware_Type:TUNNELER,Malware:SUNBRICKED,Group:Validation
d2b9c4a805c402dd697f23dd7c58a8c0	Group:Validation
d749e0f8f2cd4e14178a787571534121	Malware:PINESAP,Malware_Type:DOWNLOADER,Group:Validation
da9b5fe2fa247193830e6aef41582583	Group:Validation
dd7ab5712cd95ef787278b07b8eebb3f	Group:Validation
ddf75cc7e322d75de77b17c8ec887975	Malware_Type:TUNNELER,Malware:SUNBRICKED,Group:Validation
df9076301f1986732a3e56cd3752a29d	Malware:CORNFLAKE.V3,Group:Validation,Malware_Type:BACKDOOR
dfd94f13aa23b7fe11f88ad35f767684	Group:Validation
e0817b5012726efcc854bb396259823c	Malware:PINESAP,Group:Validation,Malware_Type:DOWNLOADER
e2022cedcea9b5ea81764996732a9880	Malware:SUNBRICKED,Malware_Type:LAUNCHER,Group:Validation
e37c5ba4fa988f7d862accfa684edfa1	Malware:PRINTSPOOFER,Group:Validation
e4beeb5f13a78d5e00e1e6697ce9d5fe	Group:Validation
e5db3d37cbbad6088f3d7d155a9599b9	Malware:PINESAP,Malware_Type:DOWNLOADER,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
e89a8674af72d6cee28e5c2043a28961	Group:Validation
ea3d4e7b3c3e959dc3ec493e3465d5ef	Group:Validation
ea7648dc7bc5c8a27a702509f5c3e964	Group:Validation
ecfd9cc2f811eb10f8b6ec8e1d350e42	Malware:LOGMEIN,Group:Validation
f1402bab6f695b14e1ca6a36439a5d33	Group:Validation
f38b46a401998845d37829054e765bce	Malware:LOGMEIN,Group:Validation
f4b90042d7f5128ccad69db79c38019f	Malware:PINESAP,Malware_Type:DOWNLOADER,Group:Validation
f4c2f6ee28ccc54b9b1e4629e1a69513	Malware_Type:DOWNLOADER,Malware:PLYCHIP,Group:Validation
fd215be6c39e6bab7d25110bc2acfcc6	Group:Validation
fdd9acd44563524fc2255b8e8f31313e	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.