Mandiant

VHR20261118 - NOVEMBER 18, 2026

The Mandiant Intelligence Validation Research Team (VRT) has published VHR20261118 - 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

- 125 Actions added
- 120 Files added

Release Highlights

- A new Action covering **Campaign 26-101** (https://advantage.mandiant.com/campaigns/CAMP.26.101), a supply chain compromise campaign by **UNC7017** (https://advantage.mandiant.com/actors/UNC7017) leveraging **SHINYROAD** (https://advantage.mandiant.com/malware/SHINYROAD) and **ADAPTAGENT** (https://advantage.mandiant.com/malware/ADAPTAGENT) payloads.
- A new Action covering **Campaign 26-038** (https://advantage.mandiant.com/campaigns/CAMP.26.038), a campaign by **UNC6722** (https://advantage.mandiant.com/actors/UNC6722) leveraging Microsoft Teams phishing and **GLASSTIDE** (https://advantage.mandiant.com/malware/GLASSTIDE) to deploy **INC** (https://advantage.mandiant.com/malware/INC) ransomware.
- A new Action demonstrating **Campaign 26-134** (https://advantage.mandiant.com/campaigns/CAMP.26.134), a campaign distributing **SILVERROOK** (https://advantage.mandiant.com/malware/SILVERROOK) and **VIDAR** (https://advantage.mandiant.com/malware/VIDAR) malware via removable media lures and process injection.
- A new Action covering **Campaign 26-166** (https://advantage.mandiant.com/campaigns/CAMP.26.166), a campaign by an actor of unknown motivations leveraging trojanized Cursor extensions for multi-platform SSH access.
- New Actions demonstrating **Campaign 26-163** (https://advantage.mandiant.com/campaigns/CAMP.26.163), a suspected Russian espionage actor **UNC7073** (https://advantage.mandiant.com/actors/UNC7073) campaign compromising MDaemon servers and deploying **OAKPULSE.A** (https://advantage.mandiant.com/malware/OAKPULSE.A) and **SWIFTECHO** (https://advantage.mandiant.com/malware/SWIFTECHO) backdoors, potentially exploiting **CVE-2025-8088** (https://advantage.mandiant.com/vulnerabilities/CVE-2025-8088).
- A new Action demonstrating **Campaign 26-171** (https://advantage.mandiant.com/campaigns/CAMP.26.171), an actor **UNC7296** (https://advantage.mandiant.com/actors/UNC7296) deploying **NODEREMOTE** (https://advantage.mandiant.com/malware/NODEREMOTE), **PINECLAY** (https://advantage.mandiant.com/malware/PINECLAY), and **SWIFTRAY** (https://advantage.mandiant.com/malware/SWIFTRAY).
- A new Action covering **CVE-2026-109618** (https://advantage.mandiant.com/vulnerabilities/CVE-2026-109618), a PHP Out-of-Memory Bailout State Corruption Vulnerability.
- New Actions demonstrating **Campaign 26-170** (https://advantage.mandiant.com/campaigns/CAMP.26.170), an unknown threat actor campaign distributing **VALLEYRAT** (https://advantage.mandiant.com/malware/VALLEYRAT) and **WINDSTRIKE** (https://advantage.mandiant.com/malware/WINDSTRIKE) malware via messaging apps and leveraging Polygon blockchain EtherHiding for C2.
- New Actions detailing **Campaign 26-127** (https://advantage.mandiant.com/campaigns/CAMP.26.127), a China-Nexus espionage campaign by **UNC6266** (https://advantage.mandiant.com/actors/UNC6266) leveraging **TRACKSTOMP** (https://advantage.mandiant.com/malware/TRACKSTOMP) and **EMPTYROAD** (https://advantage.mandiant.com/malware/EMPTYROAD) malware to target Windows and Linux systems.
- New Actions covering **CVE-2026-109619** (https://advantage.mandiant.com/vulnerabilities/CVE-2026-109619), known as **PHP2Shell** (https://advantage.mandiant.com/vulnerabilities/CVE-2026-109619), a PHP Cross-Request Stale Global State Use-After-Free vulnerability that allows a remote attacker to execute arbitrary code and has been confirmed to be

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

exploited in the wild.

- New Actions demonstrating **Campaign 26-137** (https://advantage.mandiant.com/campaigns/CAMP.26.137), involving unknown threat actor **UNC7129** (https://advantage.mandiant.com/actors/UNC7129) leveraging **GREYMOON** (https://advantage.mandiant.com/malware/GREYMOON) JavaScript on compromised sites and ClickFix social engineering to launch PowerShell payloads.

New Actions

A total of 125 Actions have been added to the content baseline with this update. This includes 125 Network Actions. All Actions in this release are tagged using the MITRE ATT&CK v13 framework.

Network Actions

VID	Name	Tags
A109-519	Malicious File Transfer - CROSSROAD, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CROSSROAD,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-520	Malicious File Transfer - UNC5720, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5720,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-521	Malicious File Transfer - UNC5720, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5720,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-522	Malicious File Transfer - UNC5720, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5720,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-523	Malicious File Transfer - UNC5720, GLOWTREE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5720,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GLOWTREE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-524	Malicious File Transfer - UNC6004, Download, Variant #2	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
A109-525	Malicious File Transfer - UNC6004, Download, Variant #3	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
A109-526	Malicious File Transfer - UNC6004, Download, Variant #4	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

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-527	Malicious File Transfer - UNC6004, Download, Variant #5	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
A109-528	Malicious File Transfer - UNC6004, Download, Variant #6	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
A109-529	Malicious File Transfer - UNC6004, FELLCROP, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6004,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FELLCROP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-530	Malicious File Transfer - UNC6266, FROSTVALE, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6266,CAMP.26.127,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FROSTVALE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-531	Malicious File Transfer - UNC6266, FROSTVALE, Download, Variant #11	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
A109-532	Malicious File Transfer - UNC6266, FROSTVALE, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6266,CAMP.26.127,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FROSTVALE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-533	Malicious File Transfer - UNC6266, FROSTVALE, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6266,CAMP.26.127,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FROSTVALE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-534	Malicious File Transfer - UNC6266, FROSTVALE, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6266,CAMP.26.127,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FROSTVALE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-535	Malicious File Transfer - UNC6266, FROSTVALE, Download, Variant #8	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
A109-536	Malicious File Transfer - UNC6266, FROSTVALE, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6266,CAMP.26.127,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FROSTVALE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-537	Malicious File Transfer - UNC6266, KRYOSTAT, Download, Variant #2	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
A109-538	Malicious File Transfer - UNC6518, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-539	Malicious File Transfer - UNC6518, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-541	Malicious File Transfer - UNC6518, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-542	Malicious File Transfer - UNC6518, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-543	Malicious File Transfer - UNC6518, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-544	Malicious File Transfer - UNC6518, Download, Variant #15	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-545	Malicious File Transfer - UNC6518, Download, Variant #16	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-546	Malicious File Transfer - UNC6518, Download, Variant #17	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,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
A109-547	Malicious File Transfer - UNC6518, Download, Variant #18	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-548	Malicious File Transfer - UNC6518, Download, Variant #19	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-549	Malicious File Transfer - UNC6518, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-551	Malicious File Transfer - UNC6518, Download, Variant #21	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-554	Malicious File Transfer - UNC6518, Download, Variant #24	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-555	Malicious File Transfer - UNC6518, Download, Variant #25	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-557	Malicious File Transfer - UNC6518, Download, Variant #27	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-558	Malicious File Transfer - UNC6518, Download, Variant #28	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-559	Malicious File Transfer - UNC6518, Download, Variant #29	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-560	Malicious File Transfer - UNC6518, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,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
A109-561	Malicious File Transfer - UNC6518, Download, Variant #30	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-562	Malicious File Transfer - UNC6518, Download, Variant #31	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-563	Malicious File Transfer - UNC6518, Download, Variant #32	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-564	Malicious File Transfer - UNC6518, Download, Variant #33	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-565	Malicious File Transfer - UNC6518, Download, Variant #34	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-566	Malicious File Transfer - UNC6518, Download, Variant #35	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-567	Malicious File Transfer - UNC6518, Download, Variant #36	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-568	Malicious File Transfer - UNC6518, Download, Variant #37	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-569	Malicious File Transfer - UNC6518, Download, Variant #38	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-570	Malicious File Transfer - UNC6518, Download, Variant #39	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,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
A109-571	Malicious File Transfer - UNC6518, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-572	Malicious File Transfer - UNC6518, Download, Variant #40	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-573	Malicious File Transfer - UNC6518, Download, Variant #41	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-574	Malicious File Transfer - UNC6518, Download, Variant #42	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-575	Malicious File Transfer - UNC6518, Download, Variant #43	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-576	Malicious File Transfer - UNC6518, Download, Variant #44	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-577	Malicious File Transfer - UNC6518, Download, Variant #45	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-578	Malicious File Transfer - UNC6518, Download, Variant #46	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-579	Malicious File Transfer - UNC6518, Download, Variant #47	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-580	Malicious File Transfer - UNC6518, Download, Variant #48	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,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
A109-581	Malicious File Transfer - UNC6518, Download, Variant #49	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-582	Malicious File Transfer - UNC6518, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-583	Malicious File Transfer - UNC6518, Download, Variant #50	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-584	Malicious File Transfer - UNC6518, Download, Variant #51	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-585	Malicious File Transfer - UNC6518, Download, Variant #52	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-586	Malicious File Transfer - UNC6518, Download, Variant #53	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-587	Malicious File Transfer - UNC6518, Download, Variant #54	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-588	Malicious File Transfer - UNC6518, Download, Variant #55	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-589	Malicious File Transfer - UNC6518, Download, Variant #56	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-591	Malicious File Transfer - UNC6518, Download, Variant #58	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,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
A109-592	Malicious File Transfer - UNC6518, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-593	Malicious File Transfer - UNC6518, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-594	Malicious File Transfer - UNC6518, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-595	Malicious File Transfer - UNC6518, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-596	Malicious File Transfer - UNC6518, XENORAT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:XENORAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-597	Malicious File Transfer - UNC6518, XENORAT, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6518,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:XENORAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-598	Malicious File Transfer - UNC6722, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6722,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-599	Malicious File Transfer - UNC6722, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6722,CAMP.26.038,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-600	Malicious File Transfer - UNC6722, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6722,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
A109-601	Malicious File Transfer - UNC6969, SANDSTICK, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6969,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDSTICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-602	Malicious File Transfer - UNC6969, SANDSTICK, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6969,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDSTICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-603	Malicious File Transfer - UNC6969, SANDSTICK, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6969,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDSTICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-604	Malicious File Transfer - UNC6969, SANDSTICK, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6969,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDSTICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-606	Malicious File Transfer - UNC6969, SANDSTICK, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6969,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDSTICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-607	Malicious File Transfer - UNC6969, SANDSTICK, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6969,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDSTICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-608	Malicious File Transfer - UNC6969, SANDSTICK, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6969,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDSTICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-609	Malicious File Transfer - UNC6969, SANDSTICK, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6969,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDSTICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-610	Malicious File Transfer - UNC6969, SANDSTICK, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6969,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDSTICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-612	Malicious File Transfer - UNC6969, SANDSTICK, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6969,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDSTICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-613	Malicious File Transfer - UNC6969, SANDSTICK, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6969,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDSTICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-614	Malicious File Transfer - UNC6969, SANDSTICK, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6969,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDSTICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-615	Malicious File Transfer - UNC7017, CROSSROAD, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7017,CAMP.26.101,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CROSSROAD,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-616	Malicious File Transfer - UNC7073, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7073,CAMP.26.163,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-617	Malicious File Transfer - UNC7073, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7073,CAMP.26.163,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-618	Malicious File Transfer - UNC7073, OAKPULSE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7073,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:OAKPULSE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-619	Malicious File Transfer - UNC7073, PINEFROST, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7073,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PINEFROST,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-620	Malicious File Transfer - UNC7073, SWIFTECHO, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7073,CAMP.26.163,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SWIFTECHO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-621	Malicious File Transfer - UNC7073, SWIFTECHO, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7073,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SWIFTECHO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-622	Malicious File Transfer - UNC7113, SILVERROOK, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7113,CAMP.26.134,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SILVERROOK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-623	Malicious File Transfer - UNC7129, GREYMOON, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7129,CAMP.26.137,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYMOON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-624	Malicious File Transfer - UNC7129, GREYMOON, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7129,CAMP.26.137,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYMOON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-625	Malicious File Transfer - UNC7129, GREYMOON, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7129,CAMP.26.137,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYMOON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-626	Malicious File Transfer - UNC7129, GREYMOON, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7129,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYMOON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-627	Malicious File Transfer - UNC7129, GREYMOON, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7129,CAMP.26.137,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GREYMOON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-628	Malicious File Transfer - UNC7163, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7163,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-629	Malicious File Transfer - UNC7204, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7204,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-630	Malicious File Transfer - UNC7204, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7204,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-631	Malicious File Transfer - UNC7204, SCREENCONNECT, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7204,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SCREENCONNECT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-632	Malicious File Transfer - UNC7204, SCREENCONNECT, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7204,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SCREENCONNECT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-633	Malicious File Transfer - UNC7204, SCREENCONNECT, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7204,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SCREENCONNECT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-634	Malicious File Transfer - UNC7245, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7245,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-635	Malicious File Transfer - UNC7245, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7245,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
A109-636	Malicious File Transfer - UNC7245, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7245,CAMP.26.170,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-637	Malicious File Transfer - UNC7245, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7245,CAMP.26.170,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-638	Malicious File Transfer - UNC7245, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7245,CAMP.26.170,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-639	Malicious File Transfer - UNC7245, JADETRAIL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7245,CAMP.26.170,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:JADETRAIL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-640	Malicious File Transfer - UNC7245, VALLEYRAT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7245,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VALLEYRAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-641	Malicious File Transfer - UNC7245, VALLEYRAT, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7245,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VALLEYRAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-642	Malicious File Transfer - UNC7245, WINDSTRIKE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7245,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WINDSTRIKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-643	Malicious File Transfer - UNC7245, WINDSTRIKE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7245,CAMP.26.170,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WINDSTRIKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-644	Malicious File Transfer - UNC7245, WINDSTRIKE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7245,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:WINDSTRIKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-645	Malicious File Transfer - UNC7266, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7266,CAMP.26.166,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-646	Malicious File Transfer - UNC7296, NODEREMOTE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7296,CAMP.26.171,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NODEREMOTE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-647	Phishing Email - Malicious Attachment, UNC7073, 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:UNC7073,CAMP.26.163,Control:Email,NIST:CM-7,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A109-648	Application Vulnerability - CVE-2026-109618, Variant #2	ATT&CK:Command and Control,ATT&CK:Execution,ATT&CK:Initial Access,ATT&CK:M1016,ATT&CK:M1026,ATT&CK:M1030,ATT&CK:M1048,ATT&CK:M1050,ATT&CK:M1051,ATT&CK:T1071.001,ATT&CK:T1190,ATT&CK:T1203,CVE-2026-109618,CWE:119,CWE:89,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,NIST:CM-5,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A109-649	Application Vulnerability - CVE-2026-109619, Variant #2	ATT&CK:Command and Control,ATT&CK:Execution,ATT&CK:Initial Access,ATT&CK:M1016,ATT&CK:M1026,ATT&CK:M1030,ATT&CK:M1048,ATT&CK:M1050,ATT&CK:M1051,ATT&CK:T1071.001,ATT&CK:T1190,ATT&CK:T1203,CVE-2026-109619,CWE:119,CWE:89,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,NIST:CM-5,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A109-650	Application Vulnerability - CVE-2026-109619, Variant #1	ATT&CK:Command and Control,ATT&CK:Execution,ATT&CK:Initial Access,ATT&CK:M1016,ATT&CK:M1026,ATT&CK:M1030,ATT&CK:M1048,ATT&CK:M1050,ATT&CK:M1051,ATT&CK:T1071.001,ATT&CK:T1190,ATT&CK:T1203,CVE-2026-109619,CWE:119,CWE:89,Control:NGFW,Control:Proxy,Control:WAF,NIST:CM-5,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-651	Application Vulnerability - CVE-2026-109618, Variant #1	ATT&CK:Command and Control,ATT&CK:Execution,ATT&CK:Initial Access,ATT&CK:M1016,ATT&CK:M1026,ATT&CK:M1030,ATT&CK:M1048,ATT&CK:M1050,ATT&CK:M1051,ATT&CK:T1071.001,ATT&CK:T1190,ATT&CK:T1203,CVE-2026-109618,CWE:119,CWE:89,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,NIST:CM-5,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted

New Files

A total of 120 new files have been added to the File Library with this update.This includes 120 malicious files.

Malicious Files

File MD5	Tags
033f895343ecbffcbe8b9bc0cba39879	Group:Validation
0541e78739c29579f9266daaada067ba	Group:Validation
0821cd605eb8bf5541bc300c853c837b	Group:Validation
096324d7fdcc8827c4d9176da5a23191	Malware:SANDSTICK,Malware_Type:DROPPER,Group:Validation
09a41c6692a2b33832057d32b5c84de5	Malware:FROSTVALE,Malware_Type:BACKDOOR,Group:Validation
0a903cd35596887dfa3a798208d8729d	Group:Validation
0bae93b9912486f3aee1366c324cc927	Group:Validation
10344bab93bba45ef595360895355d83	Malware:SILVERROOK,Malware_Type:DROPPER,Group:Validation
1036639d8bf40811b228140f58468439	Malware:CROSSROAD,Malware_Type:DOWNLOADER,Group:Validation
141b70024fd6cb2b6fec4c0d2d37622b	Group:Validation
176ba482554a9c2f2864234ad0e7ec82	Malware:NODEREMOTE,Malware_Type:BACKDOOR,Group:Validation
181c408451c3b74ec4d5142c5df2fa11	Group:Validation
1c0aeffefefac554c3fb659e50424cbc	Group:Validation
1f26d283a74dbee1fb75afa9e06f3147	Group:Validation
205434c6000cca877e00275392055605	Malware:XENORAT,Malware_Type:BACKDOOR,Group:Validation
21b91e3d13f1256f2bb6d0435dd45e2a	Malware:CROSSROAD,Malware_Type:DOWNLOADER,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
22b48b25feaf9d2ad3a49c22cf483336	Group:Validation
2355241846b80acb46365901f222cbbe	Malware:WINDSTRIKE,Malware_Type:DOWNLOADER,Group:Validation
275992b399aee888eec0b2c0fbb88ef2	Group:Validation
27f0fb1c153957bae1ebb83d5bbaf4fd	Group:Validation
2ce2a1508118ea77444af31bf7e04f58	Malware:SWIFTECHO,Group:Validation
2f2fb76fbb6280b2e4c6c5ab930110ca	Malware:SANDSTICK,Malware_Type:DROPPER,Group:Validation
2f9bcb263a5e6a2bbb5841fdb4323ea1	Group:Validation
309084c49dd4b4efc63b30e71fe87195	Group:Validation
330eff80a17ae8672ac5f8f0eb95e970	Group:Validation
38300e1d929982477a764e601ad8c959	Malware:SCREENCONNECT,Group:Validation
398dfbd832899e1a6421ab94a7800976	Malware:FROSTVALE,Malware_Type:BACKDOOR,Group:Validation
39df04c18ddf4ab33d918ff8bdf14d88	Malware:SANDSTICK,Malware_Type:DROPPER,Group:Validation
3b22588615a1f2a75d192d2598fdd88f	Group:Validation
3b52411202288830c092ad8296c4e07c	Group:Validation
3b5a459f999ddaa1dcfff112572fd1f3	Malware_Type:LAUNCHER,Group:Validation
3c5efc2b162c28aedf21c0f5856d3b07	Group:Validation
416b7232b20312bcd27441154b5b2d53	Group:Validation
41c4c538887021925260943cdecba8e2	Malware:FROSTVALE,Malware_Type:BACKDOOR,Group:Validation
422b052e980998735e4741609f5c93f7	Group:Validation
4408080531de05a347584acbb1b5d8d9	Group:Validation
45e9946cd3e192b0ffc662d63782b6cc	Malware:SANDSTICK,Malware_Type:DROPPER,Group:Validation
462051e85ba765b15a7f0cf9cc33635f	Group:Validation
4714876dd449ed4e1f11ff517d13a9ca	Malware:SCREENCONNECT,Group:Validation
4a28831d52881242b6ceae552cd61ab9	Malware:FROSTVALE,Malware_Type:BACKDOOR,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
4a89fa5c97327ba9245e4516d432927c	Group:Validation,Malware:SANDSTICK,Malware_Type:DROPPER
4c7292275b41ebf411c04ac8b1b41011	Group:Validation
52c28e3cfe3acf0c78203752f41c0cf9	Group:Validation
561518ccafe187d72b0bf86ab8c132a1	Malware_Type:DROPPER,Group:Validation,Malware:SANDSTICK
5660f87eef59ed7602f1eb9c2270be0d	Group:Validation
5731d2747808cb32a2ee44cb4e5acb1c	Malware:FROSTVALE,Malware_Type:BACKDOOR,Group:Validation
585182e1e22ee2b0957923a5873ded88	Group:Validation
59526ca4176073163d8a55df7872fb04	Malware:GREYMOON,Malware_Type:DOWNLOADER,Group:Validation
5963e6bf6ec0b270eed4ac4dddfefc42	Group:Validation,Malware:FROSTVALE,Malware_Type:BACKDOOR
59d1d7d8a46e957f0c1e6162828845a9	Malware:GLOWTREE,Malware_Type:BACKDOOR,Group:Validation
5c87f94763a518be09d3566aadc611d3	Malware:SANDSTICK,Malware_Type:DROPPER,Group:Validation
5ce99602fd924e27c9679809074a6ba7	Malware:SCREENCONNECT,Group:Validation
6560149c214f9d443ad8798d76f4f1bb	Group:Validation
66f9d2d3a8f7c1c2c415507aa080f418	Group:Validation
68fa512a71ab9b298aa28f87e6554eb1	Malware:PINEFROST,Malware_Type:UTILITY,Group:Validation
69c98150cc6aad0a91714d5dd4b36544	Malware:FELLCROP,Malware_Type:BACKDOOR,Group:Validation
6b5efd6d999bece9840667fe2a455e35	Malware:FROSTVALE,Malware_Type:BACKDOOR,Group:Validation
6cf0d2d0df8483c81b8ab00e10127398	Group:Validation
70048f5db71efaaadac4cc05a2f72e2b	Group:Validation,Malware:GREYMOON,Malware_Type:DOWNLOADER
757001e57c058117f448ac6deb4c26c3	Group:Validation
759b9a3ad2811c5178421a19ad458a75	Group:Validation
7a698b5f277f1e3c1f83b9a565f3bc24	Malware_Type:LAUNCHER,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
7be35e6c7bf077950b641020d886d59f	Group:Validation
7d6238048e60393d0597e7f1cae7f328	Group:Validation
7f4c0c82301b9da05c5730cfbc042dfd	Group:Validation
80af7328923bbe2fbbbf79e2151cec5a	Group:Validation
81e2583e101af38450984c557411c515	Malware:JADETRAIL,Malware_Type:LAUNCHER,Group:Validation
8255e1377d4301ad2624d74cae4c955f	Group:Validation
850ec3bfe0c7e6fce09e5a17f257c84c	Malware:SANDSTICK,Malware_Type:DROPPER,Group:Validation
8c17b95bcc43f96e21ef46d78bf98479	Group:Validation
8cd7a49644c33cdcf91304ad616f7cef	Malware_Type:DOWNLOADER,Group:Validation,Malware:WINDSTRIKE
8d335ec4439fc2a210092a00f16629fc	Group:Validation
8de5342f49967789bb63a0047d6b50ae	Group:Validation
90cc548d728a8d15b9bd3266ae5e58c6	Group:Validation
96663e2cbb651fee6644dd5b4c46ce19	Group:Validation
984c2347051e6cc535fed67132c1a4ea	Group:Validation
996a602f46353347a2ff8ba145d82c2a	Group:Validation
99a03ade723e860ee08cd79d15492e84	Malware:SANDSTICK,Group:Validation,Malware_Type:DROPPER
9cdf52cc1dcafd261e008f60559f1d76	Group:Validation
9e6f9b4241c5a6fa842ca911270569b6	Malware:OAKPULSE,Malware_Type:BACKDOOR,Group:Validation
a13cc9c6b0d89f1bdb88ded135f05b0c	Group:Validation
a533d6332709bcbdbdd90642546e0448	Malware:VALLEYRAT,Malware_Type:BACKDOOR,Group:Validation
afdea5736dc2530ee7ddaa7147e87a13	Group:Validation
afe11bdaf1b9a20d09b93ee751a62fd0	Group:Validation
b2583144a4c23677f7c33b1bfc9291a1	Group:Validation
b51d5ebb9aed9d139081d15d9cbbda95	Malware:XENORAT,Malware_Type:BACKDOOR,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
b56ba68b7b6b53825a1cecbb25e15439	Group:Validation
b889a30e76fb8b5c6e887effce9068d4	Group:Validation
b90f8aa5d260094e3333928fadc743c4	Malware_Type:CRYPTOCURRENCY_MINER,Group:Validation
ba37cb88475142dd7b7a83c130d01b06	Group:Validation
ba6fa0d425be19817f6eaf9e23ff9757	Malware_Type:INSTALLER,Group:Validation
c2dd1d076bc04c2e9268c92341b78d4f	Malware:GREYMOON,Malware_Type:DOWNLOADER,Group:Validation
c3f8e9f39bd958450e03c353edba8a0d	Group:Validation
c42708354261ac78983d305d826fde53	Group:Validation
c685e810b6bd7adb00a515a9db1b5df9	Group:Validation
c712f2ca3abd80fa8751af7c6d9b1732	Malware:WINDSTRIKE,Malware_Type:DOWNLOADER,Group:Validation
cbdd6537250b6a94846cdb212ad7bc77	Group:Validation
cc688731139e7a622ec54255727e34ce	Group:Validation
d8e1eb4966ce67e0bb6221603499642f	Malware:SANDSTICK,Malware_Type:DROPPER,Group:Validation
db64cc32d8785809cb950dec4eac05b4	Malware:GREYMOON,Malware_Type:DOWNLOADER,Group:Validation
dc6974ba65edb08b32eee02b57eaf4c4	Malware:SWIFTECHO,Malware_Type:BACKDOOR,Group:Validation
dd20eedf930e6d9fae11f4b85a4e89bb	Group:Validation
ddf31825d791709631bf41d54a25f70e	Group:Validation
e048ce27e87e201d8e07a04d95be3dd2	Group:Validation
e1799dd76ad710a509114da79f1e4def	Group:Validation
e1803b02dfba80b4f2c16bf62d148fb4	Group:Validation
e36e162f3e8fd3767816a3bd572401a0	Group:Validation
e3d36d0a7ea12a139cf97255249d29d6	Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
e92ca354345e1cdbac574e5c7109d724	Malware:GREYMOON,Malware_Type:DOWNLOADER,Group:Validation
ea8df00027c611ad155a06e19ffc73a8	Malware:SANDSTICK,Malware_Type:DROPPER,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
ecac84d11eaedc3663c93abaabd05731	Group:Validation
f06368b347da5b5f6f05aa39bc5906a1	Group:Validation
f07f729076d5dc83557995acd1f689a7	Group:Validation
f300a5928f6b193e12203440f9a96eb8	Malware:KRYOSTAT,Malware_Type:BACKDOOR,Group:Validation
f49bcd657ef1e626e85ce858958c1769	Malware_Type:BACKDOOR,Group:Validation
fcce762dc213cf8353e6189c94972676	Group:Validation
fce5ce18307d576f59ed616408c1f0f7	Group:Validation
fd7de91cb5d88ce71455fe588c4c7793	Malware:SANDSTICK,Malware_Type:DROPPER,Group:Validation
fd9ee6daf6818ee44d57e3f225dbd993	Group:Validation
fdee31f8e8d689802da0a1e42d0171fd	Malware:VALLEYRAT,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.