Mandiant

VHR20261021 - OCTOBER 21, 2026

The Mandiant Intelligence Validation Research Team (VRT) has published VHR20261021 - 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

- 101 Actions added
- 90 Files added

Release Highlights

- New Actions demonstrating **Campaign 26-141** (https://advantage.mandiant.com/campaigns/CAMP.26.141), an unknown motivated actor campaign leveraging fraudulent IT support phishing and PowerShell cradles to deploy the **WINDCHART** (https://advantage.mandiant.com/malware/WINDCHART) backdoor.
- New Actions demonstrating **Campaign 22-009** (https://advantage.mandiant.com/campaigns/CAMP.22.009), where **APT19** (https://advantage.mandiant.com/actors/APT19) exploits **CVE-2021-44228** (https://advantage.mandiant.com/vulnerabilities/CVE-2021-44228) to deploy **COLDSTEEL** (https://advantage.mandiant.com/malware/COLDSTEEL) at primarily Asian-based organizations.
- New Action demonstrating **Campaign 26-017** (https://advantage.mandiant.com/campaigns/CAMP.26.017), where **UNC6713** (https://advantage.mandiant.com/actors/UNC6713) deploys **NEONSLIDE** (https://advantage.mandiant.com/malware/NEONSLIDE) via ClickFix lures with scheduled task persistence and Defender evasion.
- New Actions 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) via removable media lures and process injection.
- New Actions demonstrating **Campaign 26-148** (https://advantage.mandiant.com/campaigns/CAMP.26.148), an unknown threat actor's campaign delivering archive lures via Microsoft Teams phishing to execute **DIRTDISC** (https://advantage.mandiant.com/malware/DIRTDISC) payloads via DLL search order hijacking.
- New Actions demonstrating **Campaign 26-146** (https://advantage.mandiant.com/campaigns/CAMP.26.146), a financially motivated campaign leveraging ClickFix lures, fileless PowerShell scripts, and homoglyph-obfuscated MSIExec commands to deploy **LONESCOOT** (https://advantage.mandiant.com/malware/LONESCOOT), **MOONDUST** (https://advantage.mandiant.com/malware/MOONDUST), and **SLOWRISE** (https://advantage.mandiant.com/malware/SLOWRISE).
- A new Action demonstrating **Campaign 26-093** (https://advantage.mandiant.com/campaigns/CAMP.26.093), a campaign by **UNC6984** (https://advantage.mandiant.com/actors/UNC6984) that targets infrastructure utilizing IIS web shells and token impersonation, and uses **PRINTSPOOFER** (https://advantage.mandiant.com/malware/PRINTSPOOFER) malware and the **WHOAMI** (https://advantage.mandiant.com/malware/WHOAMI) tool.
- New Actions demonstrating **Campaign 26-149** (https://advantage.mandiant.com/campaigns/CAMP.26.149), a suspected Initial Access Broker campaign leveraging malicious archives and DLL side-loading to deliver **BLUESHIFT** (https://advantage.mandiant.com/malware/BLUESHIFT), **REMCOS** (https://advantage.mandiant.com/malware/REMCOS), and **XWORM** (https://advantage.mandiant.com/malware/XWORM).
- New Actions demonstrating **Campaign 26-145** (https://advantage.mandiant.com/campaigns/CAMP.26.145) by unknown espionage actor **UNC7160** (https://advantage.mandiant.com/actors/UNC7160) exploiting **CVE-2026-88772** (https://advantage.mandiant.com/vulnerabilities/CVE-2026-88772) to deploy **WHIPSHOT** (https://advantage.mandiant.com/malware/WHIPSHOT) webshells and **SLAPSHOT** (https://advantage.mandiant.com/malware/SLAPSHOT) proxy tunnels for data theft.
- A new Action covering **Campaign 26-156** (https://advantage.mandiant.com/campaigns/CAMP.26.156), detailing how

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

UNC7204 (https://advantage.mandiant.com/actors/UNC7204) deploys **SCREENCONNECT** (https://advantage.mandiant.com/malware/SCREENCONNECT) backdoors via phishing lures and malicious scripts.

- New Actions covering **Campaign 26-157** (https://advantage.mandiant.com/campaigns/CAMP.26.157), a suspected PRC-nexus actor campaign targeting Philippines defense and government entities by leveraging **DUSKWING** (https://advantage.mandiant.com/malware/DUSKWING) and exploiting **CVE-2026-96951** (https://advantage.mandiant.com/vulnerabilities/CVE-2026-96951).
- New Actions demonstrating **Campaign 26-158** (https://advantage.mandiant.com/campaigns/CAMP.26.158), an espionage-motivated actor **UNC5720** (https://advantage.mandiant.com/actors/UNC5720) leveraging phishing and DLL side-loading to deploy the **GLOWTREE** (https://advantage.mandiant.com/malware/GLOWTREE) backdoor.
- New Actions demonstrating **Campaign 26-159** (https://advantage.mandiant.com/campaigns/CAMP.26.159), where an actor of unknown motivations deploys masqueraded **MESHAGENT** (https://advantage.mandiant.com/malware/MESHAGENT) via **COASTWIND** (https://advantage.mandiant.com/malware/COASTWIND) dropper for persistent C2.
- New Actions demonstrating **Campaign 26-151** (https://advantage.mandiant.com/campaigns/CAMP.26.151), an unknown threat group leveraging WhatsApp social engineering attacks to deploy VBScript payloads and WHQL-signed drivers.
- A new Action covering **CVE-2026-88771** (https://advantage.mandiant.com/vulnerabilities/CVE-2026-88771), a Command Injection vulnerability that allows a remote attacker to execute arbitrary code with root privileges.
- A new Action covering **CVE-2026-104935** (https://advantage.mandiant.com/vulnerabilities/CVE-2026-104935), an Authentication Bypass by Spoofing vulnerability that allows a remote attacker to execute arbitrary code.
- New Actions demonstrating **Campaign 26-153** (https://advantage.mandiant.com/campaigns/CAMP.26.153) where the actor **UNC7194** (https://advantage.mandiant.com/actors/UNC7194) of unknown motivations exploited **CVE-2026-88771** (https://advantage.mandiant.com/vulnerabilities/CVE-2026-88771) for initial access and persistence via a PHP webshell.

New Actions

A total of 101 Actions have been added to the content baseline with this update. This includes 101 Network Actions. All Actions in this release are tagged using the MITRE ATT&CK v13 framework.

Network Actions

VID	Name	Tags
A109-414	Application Vulnerability - CVE-2026-104935, Variant #1	ATT&CK:Command and Control,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,CVE-2026-104935,CWE:89,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A109-415	Application Vulnerability - CVE-2026-88771, Variant #1	ATT&CK:Command and Control,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,CVE-2026-88771,CWE:89,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A109-416	Command and Control - UNC3612, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:T1071.001,Actor:UNC3612,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.21.005,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-417	Command and Control - UNC5720, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:T1071.001,Actor:UNC5720,CAMP.26.158,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-418	Command and Control - UNC5720, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:T1071.001,Actor:UNC5720,CAMP.26.158,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-419	Command and Control - UNC6713, Registration, Variant #2	ATT&CK:Command and Control,ATT&CK:T1071.001,Actor:UNC6713,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.009,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-420	Command and Control - UNC7144, NOCKPIN, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:T1071.001,Actor:UNC7144,CAMP.26.141,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NOCKPIN,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-421	Malicious File Transfer - APT19, COLDSTEEL, Download, Variant #27	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT19,CAMP.22.009,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:COLDSTEEL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-422	Malicious File Transfer - APT19, COLDSTEEL, Download, Variant #28	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:APT19,CAMP.22.009,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:COLDSTEEL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-423	Malicious File Transfer - ATERA, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATERA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-424	Malicious File Transfer - FIN11, ROGUEJNDI, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN11,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ROGUEJNDI,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-425	Malicious File Transfer - HIDEUL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.156,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HIDEUL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-426	Malicious File Transfer - KAITEN, Download, Variant #15	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:KAITEN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-427	Malicious File Transfer - NETSCAN, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NETSCAN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-428	Malicious File Transfer - OXEEYE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:OXEEYE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-429	Malicious File Transfer - PLATYPUS, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PLATYPUS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-430	Malicious File Transfer - PLATYPUS, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PLATYPUS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-431	Malicious File Transfer - PLATYPUS, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PLATYPUS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-432	Malicious File Transfer - SILVEROAK, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.148,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SILVEROAK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-433	Malicious File Transfer - UNC2448, CUDDLEPUG, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2448,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CUDDLEPUG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-434	Malicious File Transfer - UNC2448, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2448,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-435	Malicious File Transfer - UNC2448, TUNNELFISH, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2448,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TUNNELFISH,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-436	Malicious File Transfer - UNC2448, TUNNELFISH, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2448,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TUNNELFISH,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-437	Malicious File Transfer - UNC2448, TUNNELFISH, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2448,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TUNNELFISH,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-438	Malicious File Transfer - UNC2666, UNC3005, UNC3498, REDSONJA, REDSONJA.KINSING, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2666,Actor:UNC3005,Actor:UNC3498,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REDSONJA,Malware:REDSONJA.KINSING,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-439	Malicious File Transfer - UNC3007, XMRIG, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3007,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:XMRIG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-440	Malicious File Transfer - UNC3498, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3498,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-441	Malicious File Transfer - UNC3498, REDWIND, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3498,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REDWIND,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-442	Malicious File Transfer - UNC3498, REDWIND, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3498,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REDWIND,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-443	Malicious File Transfer - UNC3510, EMP3R0R, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3510,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EMP3R0R,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-444	Malicious File Transfer - UNC3515, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3515,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
A109-445	Malicious File Transfer - UNC3516, PLAYFULGHOST, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3516,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PLAYFULGHOST,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-446	Malicious File Transfer - UNC3569, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3569,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-447	Malicious File Transfer - UNC3569, SIDESTEP, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3569,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SIDESTEP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-448	Malicious File Transfer - UNC3569, SIDESTEP, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3569,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SIDESTEP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-449	Malicious File Transfer - UNC3569, SIDESTEP, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3569,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SIDESTEP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-450	Malicious File Transfer - UNC3582, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3582,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-451	Malicious File Transfer - UNC3582, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3582,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-452	Malicious File Transfer - UNC3594, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3594,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-453	Malicious File Transfer - UNC3594, XMRIG, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3594,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:XMRIG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-454	Malicious File Transfer - UNC3612, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3612,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-455	Malicious File Transfer - UNC3653, XMRIG, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3653,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:XMRIG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-456	Malicious File Transfer - UNC3800, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3800,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-457	Malicious File Transfer - UNC3800, NMAP, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC3800,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NMAP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-458	Malicious File Transfer - UNC5720, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5720,CAMP.26.158,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-459	Malicious File Transfer - UNC5720, GLOWTREE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5720,CAMP.26.158,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GLOWTREE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-460	Malicious File Transfer - UNC5890, HAVOCDEMON, IRONTWISTER, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5890,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HAVOCDEMON,Malware:IRONTWISTER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-461	Malicious File Transfer - UNC5890, IRONTWISTER, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5890,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:IRONTWISTER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-462	Malicious File Transfer - UNC5890, IRONTWISTER, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5890,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:IRONTWISTER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-463	Malicious File Transfer - UNC6713, Download, Variant #7	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
A109-464	Malicious File Transfer - UNC6984, Download, Variant #2	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
A109-465	Malicious File Transfer - UNC7079, MOONDUST, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7079,CAMP.26.146,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MOONDUST,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-466	Malicious File Transfer - UNC7079, MOONDUST, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7079,CAMP.26.146,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MOONDUST,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-467	Malicious File Transfer - UNC7079, SLOWRISE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7079,CAMP.26.146,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLOWRISE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-468	Malicious File Transfer - UNC7079, SLOWRISE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7079,CAMP.26.146,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLOWRISE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-469	Malicious File Transfer - UNC7087, OVERGROW, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7087,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:OVERGROW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-470	Malicious File Transfer - UNC7113, SILVERROOK, Download, Variant #1	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

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-471	Malicious File Transfer - UNC7113, SILVERROOK, Download, Variant #2	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
A109-472	Malicious File Transfer - UNC7113, SILVERROOK, Download, Variant #3	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
A109-473	Malicious File Transfer - UNC7113, SILVERROOK, Download, Variant #4	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
A109-474	Malicious File Transfer - UNC7123, DIRTDISC, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7123,CAMP.26.148,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DIRTDISC,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-475	Malicious File Transfer - UNC7123, DIRTDISC, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7123,CAMP.26.148,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DIRTDISC,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-476	Malicious File Transfer - UNC7144, NOCKPIN, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7144,CAMP.26.141,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NOCKPIN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-477	Malicious File Transfer - UNC7144, NOCKPIN, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7144,CAMP.26.141,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NOCKPIN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-478	Malicious File Transfer - UNC7148, POLARSTAT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7148,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POLARSTAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-479	Malicious File Transfer - UNC7160, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7160,CAMP.26.145,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-480	Malicious File Transfer - UNC7160, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7160,CAMP.26.145,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-481	Malicious File Transfer - UNC7173, BLUESHIFT, REMCOS, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7173,CAMP.26.149,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUESHIFT,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-482	Malicious File Transfer - UNC7173, BLUESHIFT, XWORM, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7173,CAMP.26.149,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUESHIFT,Malware:XWORM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-483	Malicious File Transfer - UNC7173, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7173,CAMP.26.149,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-484	Malicious File Transfer - UNC7177, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7177,CAMP.26.151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-485	Malicious File Transfer - UNC7177, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7177,CAMP.26.151,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-486	Malicious File Transfer - UNC7178, GODPOTATO, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7178,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GODPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-487	Malicious File Transfer - UNC7181, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7181,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
A109-488	Malicious File Transfer - UNC7182, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7182,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-489	Malicious File Transfer - UNC7182, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7182,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-490	Malicious File Transfer - UNC7182, PLATYPUS, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7182,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PLATYPUS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-491	Malicious File Transfer - UNC7182, PLATYPUS, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7182,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PLATYPUS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-492	Malicious File Transfer - UNC7186, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7186,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-493	Malicious File Transfer - UNC7194, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7194,CAMP.26.153,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-494	Malicious File Transfer - UNC7194, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7194,CAMP.26.153,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-495	Malicious File Transfer - UNC7204, Download, Variant #1	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
A109-496	Malicious File Transfer - UNC7204, Download, Variant #2	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

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-497	Malicious File Transfer - UNC7204, Download, Variant #3	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
A109-498	Malicious File Transfer - UNC7204, SCREENCONNECT, Download, Variant #1	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
A109-499	Malicious File Transfer - UNC7204, SCREENCONNECT, Download, Variant #2	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
A109-500	Malicious File Transfer - UNC7204, SCREENCONNECT, Download, Variant #3	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
A109-501	Malicious File Transfer - UNC7204, SCREENCONNECT, Download, Variant #4	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
A109-502	Malicious File Transfer - UNC7204, SCREENCONNECT, Download, Variant #5	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
A109-503	Malicious File Transfer - UNC7207, DUSKWING, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7207,CAMP.26.157,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSKWING,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-504	Malicious File Transfer - UNC7207, DUSKWING, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7207,CAMP.26.157,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSKWING,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-505	Malicious File Transfer - UNC7213, COASTWIND, MESHAGENT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7213,CAMP.26.159,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:COASTWIND,Malware:MESHAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-506	Malicious File Transfer - UNC7213, COASTWIND, MESHAGENT, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7213,CAMP.26.159,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:COASTWIND,Malware:MESHAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-507	Malicious File Transfer - UNC7213, MESHAGENT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7213,CAMP.26.159,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MESHAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-508	Malicious File Transfer - UNC7213, MESHAGENT, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7213,CAMP.26.159,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MESHAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-509	Malicious File Transfer - UNC961, HOLEDOOR, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC961,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOLEDOOR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-510	Malicious File Transfer - VIDAR, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.134,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VIDAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-511	Malicious File Transfer - XMRIG, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:XMRIG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-512	Malicious File Transfer - XMRIG, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:XMRIG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-513	Malicious File Transfer - XMRIG, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:XMRIG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-514	Malicious File Transfer - XMRIG, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:XMRIG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

New Files

A total of 90 new files have been added to the File Library with this update.This includes 90 malicious files.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Malicious Files

File MD5	Tags
0290897724c92910ef688fd23da0b22e	Malware_Type:DROPPER,Group:Validation,Malware:BLUESHIFT,Malware:REMCOS
034a721824243c02adf3afb0d7dfb05d	Malware:PLATYPUS,Malware_Type:DOWNLOADER,Group:Validation
07112a331cc7b87ab02448a541471995	Malware:SCREENCONNECT,Group:Validation
0875f0134420a01d079f750ac3d0f738	Malware:MOONDUST,Malware_Type:DOWNLOADER,Group:Validation
08d0c6e815ac5fb188d4a775bb7f78c4	Group:Validation
10a981dfe0cd559940b511901739aa53	Group:Validation
121cb0a4765c63194c3bfc99d14ad4ce	Group:Validation
14d37b2ba441e42d5d13bd2596da3ebc	Malware:SLOWRISE,Malware_Type:DROPPER,Group:Validation
1b62070368a2f27874c5a7af3b2bafe3	Malware_Type:DROPPER,Malware:SILVERROOK,Group:Validation
1fe52c0b0139660b2335dd7b7c12ea05	Malware:XMRIG,Group:Validation
2048459854b3bfc851fb6a56a73318b3	Malware:GODPOTATO,Malware_Type:DRIVER,Group:Validation
21631ad18bf6a82ec414e157131ddf1a	Malware_Type:WEBSHELL,Group:Validation
2559e97c13e731d9f37b1630dff2bb1e	Malware_Type:CRYPTOCURRENCY_MINER,Group:Validation
27f7186499bc8d10e51d17d3d6697bc5	Malware:NETSCAN,Group:Validation
289a0109a430c5d323e50ac835a11c8d	Group:Validation
2f4b5a0d98bc4e5616f2dd04337ae674	Malware:SILVEROAK,Group:Validation
32576e48acc283ab269fac4d60bcc119	Malware:SCREENCONNECT,Group:Validation
35f77a9e5d3fcc8ae0667e18b3dafbc5	Malware:PLAYFULGHOST,Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
364abce21127495f6bf9eb6536ef28ce	Malware:XMRIG,Malware_Type:CRYPTOCURRENCY_MINER,Group:Validation
37cb911ded59254772809ba82b66dae5	Malware:NOCKPIN,Malware_Type:INSTALLER,Group:Validation
3c1aa61c1bd38bcc986628c21d0f10f5	Malware:OVERGROW,Malware_Type:BACKDOOR,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
3dfbe75871e218d08328a01c56e1bb42	Malware:REDWIND,Malware_Type:DOWNLOADER,Group:Validation
3f79e15d29855fd8a443ca06c853d328	Group:Validation
403b3fd160deaf9a9d5d9fff94f1b6e7	Malware:DIRTDISC,Malware_Type:LAUNCHER,Group:Validation
41d37c96b6e88a8bd93c119bebf21426	Group:Validation
432e9f91ee7788154fe8da0f0b7aefd1	Malware:COLDSTEEL,Malware_Type:LAUNCHER,Group:Validation
44a34e9bbaee0c0d85f21eb60b723b4e	Malware:NMAP,Group:Validation
4590ebc444b415c655f7d987dc420866	Malware:DUSKWING,Malware_Type:DOWNLOADER,Group:Validation
461f3c5677b82ebad28110a067de3445	Malware_Type:WEBSHELL,Group:Validation
4b171153bf0a462c7eb4643ad6386af6	Malware:PLATYPUS,Malware_Type:DOWNLOADER,Group:Validation
50e3da586b1003415a841c946e21b246	Malware:TUNNELFISH,Malware_Type:TUNNELER,Group:Validation
5627f5284e24f8d03abc3fead4df4727	Group:Validation
5a8dd0a1d74a096a9b0556cd9a8d5be0	Group:Validation
61186cb7d74ba929ec72dabf8bf78af7	Malware_Type:FRAMEWORK,Malware:PLATYPUS,Group:Validation
648effa354b3cbaad87b45f48d59c616	Malware:REDSONJA.KINSING,Malware_Type:BACKDOOR,Group:Validation
6b42a9f10db8b11a15006abced212fa4	Malware:ROGUEJNDI,Malware_Type:FRAMEWORK,Group:Validation
6c6bb08d6dce795bbc2f8046fc2f8626	Malware:XMRIG,Malware_Type:CRYPTOCURRENCY_MINER,Group:Validation
725db52aad17743eab033a42018c105e	Malware:HIDEUL,Group:Validation,Tool_Type:UTILITY
72c6966aeb1678235e6dfc6f53bcf7fd	Malware_Type:CRYPTOCURRENCY_MINER,Group:Validation,Malware:XMRIG
735c93dd75ebb7bf0f6179e192526ceb	Malware:SIDESTEP,Malware_Type:LAUNCHER,Group:Validation
760f70e8356140a7452d056021b6c933	Malware:SILVERROOK,Malware_Type:DROPPER,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
77b7bbd9cb255ac89f452206a0f47a2d	Malware:SILVERROOK,Malware_Type:DROPPER,Group:Validation
7af60476168bdeed25a919edf669175b	Group:Validation,Malware:CVE
7ef97450e84211f9f35d45e1e6ae1481	Malware:XMRIG,Group:Validation
7f7eba684a6b7f50e92514e864407375	Malware_Type:WEBSHELL,Group:Validation
875046b52caace5ab8f125facc3fcec2	Malware:SCREENCONNECT,Group:Validation
88a2148bed2db4abc8c04a668ad9d7d3	Malware:IRONTWISTER,Malware_Type:DROPPER,Group:Validation
8925e1792afa6a5c4e16ede2cc3a9b10	Group:Validation
8e83bcb70cb15f91a85f3d0297cad072	Malware_Type:WEBSHELL,Group:Validation
8f57ce99d53addabec1d964cd34c96f4	Malware:COLDSTEEL,Malware_Type:BACKDOOR,Group:Validation
8feb9a1c7da97b6e0d254d93da37371d	Malware:XMRIG,Group:Validation
91d9030688467775026dc84d51d13966	Malware:DUSKWING,Malware_Type:DOWNLOADER,Group:Validation
989c3c1f16c2678596b06c7b054997a4	Group:Validation,Malware_Type:DROPPER_MEMORY_ONLY,Malware:EMP3R0R
9c0a1763342046daf8b3e36b39a3d77b	Malware:SLOWRISE,Malware_Type:DROPPER,Group:Validation
9f189d85af343d731d7e776ce025580d	Malware_Type:FRAMEWORK,Group:Validation,Malware:PLATYPUS
a028948fa92594224521fcf6b6ff9c59	Malware:HAVOCDEMON,Malware:IRONTWISTER,Malware_Type:BACKDOOR,Group:Validation
a3501c3890defa102be37ce558b604ed	Group:Validation
ab22c1474c020dff823b5ebeda2dbc6a	Malware:SCREENCONNECT,Group:Validation
ac6c52632fcf8b072be3b1c5bc076fdd	Malware:POLARSTAT,Malware_Type:BACKDOOR,Group:Validation
b1e794431bc7d711a0395a54964bd065	Malware:COASTWIND,Malware:MESHAGENT,Malware_Type:DROPPER,Group:Validation
b2755fc18ae77bc86322409e82a02753	Malware:KAITEN,Malware_Type:DISRUPTION_TOOL,Group:Validation
b33a8e22a044c52742abc06f47b62547	Malware:PLATYPUS,Malware_Type:FRAMEWORK,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
ba888b713fa80bf2ed3f03ae45b36ffb	Malware:IRONTWISTER,Malware_Type:DROPPER,Group:Validation
bb724df37959c23a4ce6b5c5c374217e	Malware_Type:BACKDOOR,Group:Validation
bd3f9986f3e09b84c5fcd18055cdc12e	Malware_Type:DROPPER,Group:Validation
bde2a3c8e034d30ce13e684f324c6702	Malware:SIDESTEP,Malware_Type:LAUNCHER,Group:Validation
bee9c94f1ff6027dc8b60338f073feeb	Malware:SIDESTEP,Malware_Type:LAUNCHER,Group:Validation
c2627b27775c2d69fee340aa7c032819	Malware:GLOWTREE,Malware_Type:BACKDOOR,Group:Validation
c7d924f8b54c44e1edaa87f9b280bf39	Malware:VIDAR,Malware_Type:INSTALLER,Group:Validation
c8083b0b37507fab466b4fe092300ee1	Malware:MESHAGENT,Malware_Type:BACKDOOR,Group:Validation
c8bfafd06bfcd45d598cd39f329b25d0	Malware:SCREENCONNECT,Group:Validation
c9a4335d248ccb9733a9ba845d985ab6	Group:Validation
cacb64bdf648444e66c82f5ce61caf4b	Malware:CUDDLEPUG,Malware_Type:DOWNLOADER,Group:Validation
d403a724b8665a6e77ab09c69bd0828e	Malware:SILVERROOK,Malware_Type:DROPPER,Group:Validation
d6ae345b63833cccd0375b8230856990	Malware:BLUESHIFT,Malware:XWORM,Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
dffb306d5ce2637635da6a7da879fa6f	Malware:NOCKPIN,Malware_Type:INSTALLER,Group:Validation
e17ea3d732f8c33454cbe88eb78800ab	Malware:TUNNELFISH,Malware_Type:TUNNELER,Group:Validation
e397087edf21ad9da907b595691ce15e	Malware:XMRIG,Group:Validation
e6872486aa6eed9309d787637c287cae	Group:Validation,Malware:REDWIND,Malware_Type:DOWNLOADER
e8ddc1169e813ab3cd6a3874a7411f49	Group:Validation
ea81492f00a5aee057ab72fe7dcbbd38	Group:Validation
ebf456ca2c0d90a1b8e7bfb0b8e4ff34	Malware:DIRTDISC,Malware_Type:LAUNCHER,Group:Validation
ef391136c63a39a68bcbf48e9e55d104	Malware_Type:DOWNLOADER,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
efa3dcdf61214c784dae2b7adc9f26f8	Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
efb2cb8c321f216b2f972cc8c94b4884	Malware:MOONDUST,Group:Validation,Malware_Type:DOWNLOADER
f11bda3ded011bad816dd48a41719291	Malware:TUNNELFISH,Malware_Type:TUNNELER,Group:Validation
f4dd330ff093e69a181854eccaa2432c	Malware:HOLEDOOR,Malware_Type:BACKDOOR,Group:Validation
f8e4176e34b7601c10536415e8774542	Malware:ATERA,Group:Validation
fbe2d1eade4fce86c26ea772a7fefd04	Group:Validation
fe09cf6d3a358305f8c2f687b6f6da02	Malware:OXEEYE,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.