Mandiant

VHR20260624 - JUNE 24, 2026

The Mandiant Intelligence Validation Research Team (VRT) has published VHR20260624 - Content Expansion. This content pack requires Director version 4.14.1.0-0 or higher.

If you've enabled the Content Service, this content pack will automatically download and be applied to your Director (see **The Mandiant Content Service** (https://docs.mandiant.com/home/msv-mandiant-content-service) and **Managing Security Validation Content** (https://docs.mandiant.com/home/msv-content-settings) for full details). Otherwise, you can download the **security content pack** (https://docs.mandiant.com/home/msv-content-packs) from the Mandiant Documentation Portal.

Summary of Changes

- 370 Actions added
- 329 Files added
- 14 Actions updated
- 6 Files updated

Release Highlights

- New Actions demonstrating **Campaign 25-002** (https://advantage.mandiant.com/campaigns/CAMP.25.002), where **UNC5487** (https://advantage.mandiant.com/actors/UNC5487) conducts a social engineering campaign to deliver **REMCOS** (https://advantage.mandiant.com/malware/REMCOS) and **SHADOWLADDER** (https://advantage.mandiant.com/malware/SHADOWLADDER).
- New Actions demonstrating **Campaign 25-082** (https://advantage.mandiant.com/campaigns/CAMP.25.082), a suspected Iranian espionage threat actor **UNC1549** (https://advantage.mandiant.com/actors/UNC1549) campaign leveraging **TWOSTROKE** (https://advantage.mandiant.com/malware/TWOSTROKE) malware against Azerbaijan and Turkish-based organizations.
- A new Action covering **FLUXWEAVE** (https://advantage.mandiant.com/malware/FLUXWEAVE) leveraged in **Campaign 25-076** (https://advantage.mandiant.com/campaigns/CAMP.25.076) by **UNC6527** (https://advantage.mandiant.com/actors/UNC6527) to deliver a downloader.
- New Actions demonstrating **Campaign 25-039** (https://advantage.mandiant.com/campaigns/CAMP.25.039), a distribution cluster **UNC1543** (https://advantage.mandiant.com/actors/UNC1543) campaign leveraging **FAKEUPDATES** (https://advantage.mandiant.com/malware/FAKEUPDATES) and deceptive lures to facilitate initial access leading to ransomware and extortion.
- A new Action covering **Campaign 25-042** (https://advantage.mandiant.com/campaigns/CAMP.25.042), a North Korean Actor **UNC1069** (https://advantage.mandiant.com/actors/UNC1069) campaign employing advanced social engineering, including occasional deepfakes, to deploy macOS malware, such as **BIGMACHO** (https://advantage.mandiant.com/malware/BIGMACHO), for cryptocurrency theft.
- A new Action covering **Campaign 26-059** (https://advantage.mandiant.com/campaigns/CAMP.26.059), which involves the deployment of **VIDAR** (https://advantage.mandiant.com/malware/VIDAR) infostealer via the **NEONSLIDE** (https://advantage.mandiant.com/malware/NEONSLIDE) PowerShell downloader.
- New Actions demonstrating **Campaign 26-060** (https://advantage.mandiant.com/campaigns/CAMP.26.060), a financially motivated actor **UNC6780** (https://advantage.mandiant.com/actors/UNC6780) campaign conducting a software supply chain attack via GitHub Actions cache poisoning and deploying the **FIRESCALE** (https://advantage.mandiant.com/malware/FIRESCALE) credential stealer.
- New Actions demonstrating **Campaign 26-063** (https://advantage.mandiant.com/campaigns/CAMP.26.063), a Chinese Espionage Threat Actor campaign deploying **BADTILE** (https://advantage.mandiant.com/malware/BADTILE) and using RegSvr32 Scriptlet Bypass for execution.
- New Actions demonstrating **Campaign 26-071** (https://advantage.mandiant.com/campaigns/CAMP.26.071), an Iran-nexus threat group **UNC5795** (https://advantage.mandiant.com/actors/UNC5795) campaign conducting espionage operations against Middle Eastern targets using **HOTAIR** (https://advantage.mandiant.com/malware/HOTAIR), **AEROSTAT** (https://advantage.mandiant.com/malware/AEROSTAT), and **TREEWORLD** (https://advantage.mandiant.com/malware/TREEWORLD).

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

- A new Action covering **Campaign 26-014** (https://advantage.mandiant.com/campaigns/CAMP.26.014), a North Korea-nexus threat actor **UNC5342** (https://advantage.mandiant.com/actors/UNC5342) campaign deploying Python backdoors, including **JADESNOW** (https://advantage.mandiant.com/malware/JADESNOW), to target GitHub repositories for unauthorized code modification.
- A new Action covering **Campaign 26-072** (https://advantage.mandiant.com/campaigns/CAMP.26.072), a China-nexus financial gain actor **UNC6727** (https://advantage.mandiant.com/actors/UNC6727) deploying **SUNBRICKED** (https://advantage.mandiant.com/malware/SUNBRICKED) malware via trojanized VPN installer.
- New Actions demonstrating **Campaign 26-080** (https://advantage.mandiant.com/campaigns/CAMP.26.080), a campaign by a financially motivated actor deploying malicious LNK payloads via fake browser updates to establish persistence with **OAKSHADE** (https://advantage.mandiant.com/malware/OAKSHADE) and **RIVERSTONE** (https://advantage.mandiant.com/malware/RIVERSTONE).
- New Actions covering **UNC5669** (https://advantage.mandiant.com/actors/UNC5669), a threat cluster of unknown motivation active since July 2024 that has used social engineering tactics to gain access to networks and exfiltrate code documents.
- New Actions covering **UNC4769** (https://advantage.mandiant.com/actors/UNC4769), a financially motivated threat cluster that has monetized access via **PLAYCRYPT** (https://advantage.mandiant.com/malware/PLAYCRYPT) ransomware and frequently used **BEACON** (https://advantage.mandiant.com/malware/BEACON).
- New Actions demonstrating **Campaign 26-075** (https://advantage.mandiant.com/campaigns/CAMP.26.075), a campaign by **UNC6633** (https://advantage.mandiant.com/actors/UNC6633) that deploys **JADECLIP** (https://advantage.mandiant.com/malware/JADECLIP) malware via trojanized software to impair defenses and establish remote access, targeting entities in China and Taiwan.
- New Actions covering financially motivated threat cluster **UNC2165** (https://advantage.mandiant.com/actors/UNC2165) that deploys various ransomware families including **HADES** (https://advantage.mandiant.com/malware/HADES), **LOCKBIT** (https://advantage.mandiant.com/malware/LOCKBIT.V2), **CONTI** (https://advantage.mandiant.com/malware/CONTI), and **RANSOMHUB** (https://advantage.mandiant.com/malware/RANSOMHUB).
- A new Action covering **UNC6279** (https://advantage.mandiant.com/actors/UNC6279), a suspected Russian threat group that uses social engineering and help desk impersonation via phishing or chat platforms to establish AnyDesk sessions and deploy **VEILDRIVE** (https://advantage.mandiant.com/malware/VEILDRIVE) malware.
- New Actions covering **UNC6240** (https://advantage.mandiant.com/actors/UNC6240), a financially motivated threat cluster primarily responsible for the extortion phase of operations branded under the ShinyHunters name.
- A new Action covering **UNC6492** (https://advantage.mandiant.com/actors/UNC6492), an espionage-motivated threat cluster targeting South Korean entities in various sectors.
- New Actions covering **UNC6863** (https://advantage.mandiant.com/actors/UNC6863), a suspected China-nexus actor that has leveraged a supply chain compromise of DAEMONTOOLS to deploy **BADFALL** (https://advantage.mandiant.com/malware/BADFALL) and **SLICKDEMON** (https://advantage.mandiant.com/malware/SLICKDEMON) to compromised systems.
- New Actions covering **UNC6828** (https://advantage.mandiant.com/actors/UNC6828), a suspected Russian threat group motivated by financial gain that has been identified using a command-and-control framework dubbed “Tuk Tuk” and leveraged Anthropic’s Claude LLM to facilitate its cloud-native intrusion activities.
- A new Action covering financially motivated threat cluster **UNC5142** (https://advantage.mandiant.com/actors/UNC5142) which compromises vulnerable WordPress sites to distribute malicious payloads via **CLEARFAKE** (https://advantage.mandiant.com/malware/CLEARFAKE) malware, with observed final payloads including **AMADEY** (https://advantage.mandiant.com/malware/AMADEY) and **LUMMAC.V2** (https://advantage.mandiant.com/malware/LUMMAC.V2).
- A new Action covering **UNC6868** (https://advantage.mandiant.com/actors/UNC6868), a suspected Eastern Europe-nexus threat group leveraging malicious scripts and multi-stage downloads to deploy **SHUBSTAKE** (https://advantage.mandiant.com/malware/SHUBSTAKE) to target user credentials, browser data, and cryptocurrency assets.
- New Actions covering **BLUEBEAM** (https://advantage.mandiant.com/malware/BLUEBEAM), a publicly available webshell management tool written in JAVA, which can generate webshell payloads and has 20 built-in modules.
- New Actions covering **UNC6876** (https://advantage.mandiant.com/actors/UNC6876), a suspected Chinese cyber

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

espionage group that deploys the **HEAVYMETAL** (https://advantage.mandiant.com/malware/HEAVYMETAL) backdoor to compromise victim accounts globally.

New Actions

A total of 370 Actions have been added to the content baseline with this update. This includes 370 Network Actions. All Actions in this release are tagged using the MITRE ATT&CK v17.1 framework.

Network Actions

VID	Name	Tags
A108-756	Command and Control - CURLYGATE, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,ATT&CK:T1132,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:CURLYGATE,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-757	Command and Control - MELTRUBY, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:MELTRUBY,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-758	Command and Control - MELTRUBY, Registration, Variant #2	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MELTRUBY,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-760	Command and Control - RAMENRUMBLE, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:RAMENRUMBLE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-761	Command and Control - UNC1543, FAKEUPDATES, Check-In, Variant #4	ATT&CK:Command and Control,ATT&CK:Defense Evasion,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1040,ATT&CK:M1049,ATT&CK:M1057,ATT&CK:T1027,ATT&CK:T1041,ATT&CK:T1071.001,Actor:UNC1543,CWE:173,CWE:20,CWE:697,CWE:74,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-762	Command and Control - UNC1549, ENSYNCROLL, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ENSYNCROLL,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-763	Command and Control - UNC1549, ENSYNCROLL, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ENSYNCROLL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-764	Command and Control - UNC1549, POLLREGISTER, Registration, Variant #2	ATT&CK:Command and Control,ATT&CK:Discovery,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1082,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:POLLREGISTER,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-765	Command and Control - UNC1549, POLLREGISTER, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:POLLREGISTER,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-766	Command and Control - UNC5342, INVISIBLEFERRET, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:Discovery,ATT&CK:M1031,ATT&CK:T1016.001,ATT&CK:T1071.001,Actor:UNC5342,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:INVISIBLEFERRET,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-767	Command and Control - UNC5342, INVISIBLEFERRET, Registration, 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:INVISIBLEFERRET,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-768	Command and Control - UNC5669, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-769	Command and Control - UNC5669, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-770	Command and Control - UNC5795, AEROSTAT, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,ATT&CK:T1567.002,Actor:UNC5795,CAMP.26.071,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:AEROSTAT,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-771	Command and Control - UNC5795, Communication, Variant #2	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5795,CAMP.26.071,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-772	Command and Control - UNC5795, Communication, Variant #3	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5795,CAMP.26.071,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-773	Command and Control - UNC5795, Communication, Variant #4	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5795,CAMP.26.071,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-774	Command and Control - UNC5795, Communication, Variant #5	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5795,CAMP.26.071,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-775	Command and Control - UNC5795, Exfiltration, Variant #3	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5795,CAMP.26.071,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-776	Command and Control - UNC5795, Exfiltration, Variant #4	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,ATT&CK:T1567.002,Actor:UNC5795,CAMP.26.071,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-777	Command and Control - UNC5795, HOTAIR, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC5795,CAMP.26.071,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-778	Command and Control - UNC5795, HOTAIR, Communication, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-779	Command and Control - UNC5795, HOTAIR, Exfiltration, Variant #2	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1567.002,Actor:UNC5795,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-780	Command and Control - UNC5795, TREEWORLD, Check-In, Variant #3	ATT&CK:Command and Control,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573,Actor:UNC5795,CAMP.26.071,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TREEWORLD,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-781	Command and Control - UNC6527, FLUXWEAVE, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6527,CAMP.25.076,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:FLUXWEAVE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-782	Command and Control - UNC6633, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6633,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-783	Command and Control - UNC6699, BADTILE, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1030,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1571,Actor:UNC6699,CAMP.26.063,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-784	Command and Control - UNC6699, BADTILE, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:Defense Evasion,ATT&CK:M1021,ATT&CK:M1022,ATT&CK:M1026,ATT&CK:M1031,ATT&CK:M1037,ATT&CK:M1038,ATT&CK:M1042,ATT&CK:M1050,ATT&CK:T1071.001,ATT&CK:T1105,ATT&CK:T1218,Actor:UNC6699,CAMP.26.063,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:BADTILE,NIST:CM-11,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-785	Command and Control - UNC6828, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:Discovery,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1082,Actor:UNC6828,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-786	Command and Control - UNC6849, CHALKWIRE, VIDAR, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573,Actor:UNC6849,CAMP.26.059,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:CHALKWIRE,Malware:VIDAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-787	Command and Control - UNC6849, CHALKWIRE, VIDAR, Tasking, Variant #2	ATT&CK:Command and Control,ATT&CK:Defense Evasion,ATT&CK:M1031,ATT&CK:M1040,ATT&CK:M1049,ATT&CK:T1027,ATT&CK:T1071.001,Actor:UNC6849,CAMP.26.059,CWE:173,CWE:20,CWE:697,CWE:74,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:CHALKWIRE,Malware:VIDAR,NIST:AC-4,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-788	Command and Control - UNC6849, VIDAR, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6849,CAMP.26.059,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VIDAR,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-789	Command and Control - UNC6849, VIDAR, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:Defense Evasion,ATT&CK:M1031,ATT&CK:M1040,ATT&CK:M1049,ATT&CK:T1027,ATT&CK:T1071.001,Actor:UNC6849,CAMP.26.059,CWE:173,CWE:20,CWE:697,CWE:74,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VIDAR,NIST:AC-4,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-790	Command and Control - UNC6849, VIDAR, Telegram, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1102,Actor:UNC6849,CAMP.26.059,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VIDAR,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-791	Command and Control - UNC6923, Communication, Variant #1	ATT&CK:Command and Control,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,Actor:UNC6923,CAMP.26.080,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-11,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-792	Command and Control - UNC6923, Tasking, Variant #1	ATT&CK:Command and Control,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:T1105,Actor:UNC6923,CAMP.26.080,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-11,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-793	Malicious File Transfer - BADTILE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-794	Malicious File Transfer - BADTILE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-795	Malicious File Transfer - BADTILE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.063,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-796	Malicious File Transfer - BADTILE, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-797	Malicious File Transfer - BADTILE, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-798	Malicious File Transfer - BADTILE, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-799	Malicious File Transfer - BADTILE, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-800	Malicious File Transfer - BADTILE, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.063,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-801	Malicious File Transfer - BADTILE, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-802	Malicious File Transfer - BLUEBEAM, BLUEBEAM.ASP, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.ASP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-803	Malicious File Transfer - BLUEBEAM, BLUEBEAM.ASP, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.ASP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-804	Malicious File Transfer - BLUEBEAM, BLUEBEAM.JSP, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.JSP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-805	Malicious File Transfer - BLUEBEAM, BLUEBEAM.JSP, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.JSP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-806	Malicious File Transfer - BLUEBEAM, BLUEBEAM.JSP, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.JSP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-807	Malicious File Transfer - BLUEBEAM, BLUEBEAM.JSP, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.JSP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-808	Malicious File Transfer - BLUEBEAM, BLUEBEAM.JSP, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.JSP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-809	Malicious File Transfer - BLUEBEAM, BLUEBEAM.JSP, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.JSP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-810	Malicious File Transfer - BLUEBEAM, BLUEBEAM.JSP, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.JSP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-811	Malicious File Transfer - BLUEBEAM, BLUEBEAM.JSP, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.JSP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-812	Malicious File Transfer - BLUEBEAM, BLUEBEAM.PHP, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.PHP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-813	Malicious File Transfer - BLUEBEAM, BLUEBEAM.PHP, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.PHP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-814	Malicious File Transfer - BLUEBEAM, BLUEBEAM.PHP, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.PHP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-815	Malicious File Transfer - BLUEBEAM, BLUEBEAM.PHP, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.PHP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-816	Malicious File Transfer - BLUEBEAM, BLUEBEAM.PHP, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.PHP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-817	Malicious File Transfer - BLUEBEAM, BLUEBEAM.PHP, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.PHP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-818	Malicious File Transfer - CURLYGATE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-819	Malicious File Transfer - CURLYGATE, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-820	Malicious File Transfer - CURLYGATE, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-821	Malicious File Transfer - CURLYGATE, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-822	Malicious File Transfer - CURLYGATE, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-823	Malicious File Transfer - CURLYGATE, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-824	Malicious File Transfer - CURLYGATE, Download, Variant #15	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-825	Malicious File Transfer - CURLYGATE, Download, Variant #16	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-826	Malicious File Transfer - CURLYGATE, Download, Variant #17	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-827	Malicious File Transfer - CURLYGATE, Download, Variant #18	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-828	Malicious File Transfer - CURLYGATE, Download, Variant #19	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-829	Malicious File Transfer - CURLYGATE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-830	Malicious File Transfer - CURLYGATE, Download, Variant #20	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-831	Malicious File Transfer - CURLYGATE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-832	Malicious File Transfer - CURLYGATE, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-833	Malicious File Transfer - CURLYGATE, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-834	Malicious File Transfer - CURLYGATE, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-835	Malicious File Transfer - CURLYGATE, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-836	Malicious File Transfer - CURLYGATE, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-837	Malicious File Transfer - CURLYGATE, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CURLYGATE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-838	Malicious File Transfer - CYANSPEAR, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CYANSPEAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-839	Malicious File Transfer - CYANSPEAR, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CYANSPEAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-840	Malicious File Transfer - CYANSPEAR, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CYANSPEAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-841	Malicious File Transfer - CYANSPEAR, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CYANSPEAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-842	Malicious File Transfer - CYANSPEAR, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CYANSPEAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-843	Malicious File Transfer - CYANSPEAR, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CYANSPEAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-844	Malicious File Transfer - DUSTMAKER, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-845	Malicious File Transfer - DUSTMAKER, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-846	Malicious File Transfer - DUSTMAKER, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-847	Malicious File Transfer - DUSTMAKER, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-848	Malicious File Transfer - DUSTMAKER, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-849	Malicious File Transfer - DUSTMAKER, Download, Variant #15	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-850	Malicious File Transfer - DUSTMAKER, Download, Variant #16	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-851	Malicious File Transfer - DUSTMAKER, Download, Variant #17	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-852	Malicious File Transfer - DUSTMAKER, Download, Variant #18	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-853	Malicious File Transfer - DUSTMAKER, Download, Variant #19	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-854	Malicious File Transfer - DUSTMAKER, Download, Variant #20	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-855	Malicious File Transfer - DUSTMAKER, Download, Variant #21	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-856	Malicious File Transfer - DUSTMAKER, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-857	Malicious File Transfer - DUSTMAKER, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-858	Malicious File Transfer - DUSTMAKER, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-859	Malicious File Transfer - DUSTMAKER, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-860	Malicious File Transfer - DUSTMAKER, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-861	Malicious File Transfer - DUSTMAKER, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-862	Malicious File Transfer - DUSTMAKER, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DUSTMAKER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-863	Malicious File Transfer - EFSPOTATO, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-864	Malicious File Transfer - EFSPOTATO, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-865	Malicious File Transfer - EFSPOTATO, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-866	Malicious File Transfer - EFSPOTATO, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-867	Malicious File Transfer - EFSPOTATO, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-868	Malicious File Transfer - EFSPOTATO, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-869	Malicious File Transfer - EFSPOTATO, Download, Variant #15	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-870	Malicious File Transfer - EFSPOTATO, Download, Variant #16	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-871	Malicious File Transfer - EFSPOTATO, Download, Variant #17	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-872	Malicious File Transfer - EFSPOTATO, Download, Variant #18	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-873	Malicious File Transfer - EFSPOTATO, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-874	Malicious File Transfer - EFSPOTATO, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-875	Malicious File Transfer - EFSPOTATO, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-876	Malicious File Transfer - EFSPOTATO, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-877	Malicious File Transfer - EFSPOTATO, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-878	Malicious File Transfer - EFSPOTATO, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-879	Malicious File Transfer - EFSPOTATO, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-880	Malicious File Transfer - EFSPOTATO, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:EFSPOTATO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-881	Malicious File Transfer - JADECLIP, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:JADECLIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-882	Malicious File Transfer - KAITEN, Download, Variant #1	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
A108-883	Malicious File Transfer - KAITEN, Download, Variant #10	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
A108-884	Malicious File Transfer - KAITEN, Download, Variant #11	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
A108-885	Malicious File Transfer - KAITEN, Download, Variant #12	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
A108-886	Malicious File Transfer - KAITEN, Download, Variant #13	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
A108-887	Malicious File Transfer - KAITEN, Download, Variant #14	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
A108-888	Malicious File Transfer - KAITEN, Download, Variant #2	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
A108-889	Malicious File Transfer - KAITEN, Download, Variant #3	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
A108-890	Malicious File Transfer - KAITEN, Download, Variant #4	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

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-891	Malicious File Transfer - KAITEN, Download, Variant #5	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
A108-892	Malicious File Transfer - KAITEN, Download, Variant #6	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
A108-893	Malicious File Transfer - KAITEN, Download, Variant #7	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
A108-894	Malicious File Transfer - KAITEN, Download, Variant #8	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
A108-895	Malicious File Transfer - KAITEN, Download, Variant #9	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
A108-896	Malicious File Transfer - MASOL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MASOL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-897	Malicious File Transfer - MASOL, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MASOL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-898	Malicious File Transfer - MATANBUCHUS, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MATANBUCHUS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-899	Malicious File Transfer - MATANBUCHUS, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MATANBUCHUS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-900	Malicious File Transfer - MELTRUBY, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MELTRUBY,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-901	Malicious File Transfer - MELTRUBY, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MELTRUBY,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-902	Malicious File Transfer - MELTRUBY, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MELTRUBY,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-903	Malicious File Transfer - MELTRUBY, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MELTRUBY,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-904	Malicious File Transfer - MELTRUBY, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MELTRUBY,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-905	Malicious File Transfer - MELTRUBY, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MELTRUBY,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-906	Malicious File Transfer - MELTRUBY, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MELTRUBY,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-907	Malicious File Transfer - MELTRUBY, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MELTRUBY,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-908	Malicious File Transfer - NEONSLIDE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-909	Malicious File Transfer - NEONSLIDE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-910	Malicious File Transfer - NEONSLIDE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-911	Malicious File Transfer - NEONSLIDE, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-912	Malicious File Transfer - NEONSLIDE, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-913	Malicious File Transfer - NEONSLIDE, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-914	Malicious File Transfer - NEONSLIDE, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-915	Malicious File Transfer - NEONSLIDE, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-916	Malicious File Transfer - PEATWIRE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PEATWIRE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-917	Malicious File Transfer - PEATWIRE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PEATWIRE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-918	Malicious File Transfer - RAMENRUMBLE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:RAMENRUMBLE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-919	Malicious File Transfer - REDSONJA, REDSONJA.KINSING, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REDSONJA,Malware:REDSONJA.KINSING,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-920	Malicious File Transfer - REDSONJA, REDSONJA.KINSING, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REDSONJA,Malware:REDSONJA.KINSING,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-921	Malicious File Transfer - REDSONJA, REDSONJA.KINSING, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REDSONJA,Malware:REDSONJA.KINSING,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-922	Malicious File Transfer - REDSONJA, REDSONJA.KINSING, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REDSONJA,Malware:REDSONJA.KINSING,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-923	Malicious File Transfer - REDSONJA, REDSONJA.KINSING, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REDSONJA,Malware:REDSONJA.KINSING,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-924	Malicious File Transfer - REDSONJA, REDSONJA.KINSING, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REDSONJA,Malware:REDSONJA.KINSING,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-925	Malicious File Transfer - SANDCLOCK, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDCLOCK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-926	Malicious File Transfer - SANDCLOCK, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDCLOCK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-927	Malicious File Transfer - SANDCLOCK, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDCLOCK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-928	Malicious File Transfer - SANDCLOCK, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDCLOCK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-929	Malicious File Transfer - SANDCLOCK, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SANDCLOCK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-930	Malicious File Transfer - SHUBSTAKE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-931	Malicious File Transfer - SHUBSTAKE, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-932	Malicious File Transfer - SHUBSTAKE, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-933	Malicious File Transfer - SHUBSTAKE, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-934	Malicious File Transfer - SHUBSTAKE, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-935	Malicious File Transfer - SHUBSTAKE, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-936	Malicious File Transfer - SHUBSTAKE, Download, Variant #15	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-937	Malicious File Transfer - SHUBSTAKE, Download, Variant #16	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-938	Malicious File Transfer - SHUBSTAKE, Download, Variant #17	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-939	Malicious File Transfer - SHUBSTAKE, Download, Variant #18	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-940	Malicious File Transfer - SHUBSTAKE, Download, Variant #19	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-941	Malicious File Transfer - SHUBSTAKE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-942	Malicious File Transfer - SHUBSTAKE, Download, Variant #20	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-943	Malicious File Transfer - SHUBSTAKE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-944	Malicious File Transfer - SHUBSTAKE, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-945	Malicious File Transfer - SHUBSTAKE, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-946	Malicious File Transfer - SHUBSTAKE, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-947	Malicious File Transfer - SHUBSTAKE, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-948	Malicious File Transfer - SHUBSTAKE, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-949	Malicious File Transfer - SHUBSTAKE, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHUBSTAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-950	Malicious File Transfer - SLICKDEMON, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-951	Malicious File Transfer - SLICKDEMON, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-952	Malicious File Transfer - SLICKDEMON, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-953	Malicious File Transfer - SLICKDEMON, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-954	Malicious File Transfer - SLICKDEMON, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-955	Malicious File Transfer - SLICKDEMON, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-956	Malicious File Transfer - UNC1069, LONGWAIT, Download, Variant #17	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.25.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LONGWAIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-957	Malicious File Transfer - UNC1069, LONGWAIT, Download, Variant #22	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.25.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LONGWAIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-958	Malicious File Transfer - UNC1069, LONGWAIT, Download, Variant #23	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,CAMP.25.042,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LONGWAIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-959	Malicious File Transfer - UNC1069, SUGARLOADER, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SUGARLOADER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-960	Malicious File Transfer - UNC1069, SUGARLOADER, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1069,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SUGARLOADER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-961	Malicious File Transfer - UNC1543, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-962	Malicious File Transfer - UNC1543, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-963	Malicious File Transfer - UNC1543, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-964	Malicious File Transfer - UNC1543, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-965	Malicious File Transfer - UNC1543, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-966	Malicious File Transfer - UNC1543, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-967	Malicious File Transfer - UNC1543, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-968	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-969	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-970	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-971	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-972	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #15	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-973	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #16	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-974	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #17	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-975	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #18	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-976	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #19	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-977	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #20	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-979	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #22	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-980	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #23	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-981	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #24	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-982	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #25	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-983	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #26	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-984	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #27	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-985	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #28	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-986	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #29	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-987	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #30	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-988	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #31	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-989	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #32	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-990	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #33	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-991	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #34	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-992	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #35	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-993	Malicious File Transfer - UNC1549, ENSYNCROLL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,CAMP.25.082,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ENSYNCROLL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-994	Malicious File Transfer - UNC1549, ENSYNCROLL, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,CAMP.25.082,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ENSYNCROLL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-995	Malicious File Transfer - UNC2165, COILCAGE, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:COILCAGE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-996	Malicious File Transfer - UNC2165, COILCAGE, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:COILCAGE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-997	Malicious File Transfer - UNC2165, COILCAGE, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:COILCAGE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-998	Malicious File Transfer - UNC2165, COILCAGE, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:COILCAGE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-999	Malicious File Transfer - UNC2165, COILCAGE, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:COILCAGE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-000	Malicious File Transfer - UNC2165, COILCAGE, Download, Variant #15	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:COILCAGE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-001	Malicious File Transfer - UNC2165, COILCAGE, Download, Variant #16	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:COILCAGE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-002	Malicious File Transfer - UNC2165, COILCAGE, VIPERTUNNEL, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:COILCAGE,Malware:VIPERTUNNEL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-003	Malicious File Transfer - UNC2165, VIPERTUNNEL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VIPERTUNNEL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-004	Malicious File Transfer - UNC2165, VIPERTUNNEL, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VIPERTUNNEL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-005	Malicious File Transfer - UNC2165, VIPERTUNNEL, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VIPERTUNNEL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-006	Malicious File Transfer - UNC4769, PLAYCRYPT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC4769,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PLAYCRYPT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-007	Malicious File Transfer - UNC4769, SYSTEMBC, SYSTEMBC.V2, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC4769,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SYSTEMBC,Malware:SYSTEMBC.V2,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-008	Malicious File Transfer - UNC4769, SYSTEMBC, SYSTEMBC.V2, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC4769,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SYSTEMBC,Malware:SYSTEMBC.V2,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-009	Malicious File Transfer - UNC5142, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5142,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-010	Malicious File Transfer - UNC5342, 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,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-011	Malicious File Transfer - UNC5342, INVISIBLEFERRET, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5342,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:INVISIBLEFERRET,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-012	Malicious File Transfer - UNC5487, REMCOS, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-013	Malicious File Transfer - UNC5487, REMCOS, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-014	Malicious File Transfer - UNC5487, REMCOS, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-015	Malicious File Transfer - UNC5487, REMCOS, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-016	Malicious File Transfer - UNC5487, REMCOS, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-017	Malicious File Transfer - UNC5487, REMCOS, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-018	Malicious File Transfer - UNC5487, REMCOS, Download, Variant #15	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-019	Malicious File Transfer - UNC5487, REMCOS, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-020	Malicious File Transfer - UNC5487, REMCOS, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-021	Malicious File Transfer - UNC5487, REMCOS, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-022	Malicious File Transfer - UNC5487, REMCOS, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-023	Malicious File Transfer - UNC5487, REMCOS, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-024	Malicious File Transfer - UNC5487, REMCOS, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-025	Malicious File Transfer - UNC5487, REMCOS, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-026	Malicious File Transfer - UNC5487, REMCOS, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-027	Malicious File Transfer - UNC5487, REMCOS, SHADOWLADDER, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,Malware:SHADOWLADDER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-028	Malicious File Transfer - UNC5487, REMCOS, SHADOWLADDER, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,Malware:SHADOWLADDER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-029	Malicious File Transfer - UNC5487, REMCOS, SHADOWLADDER, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,Malware:SHADOWLADDER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-030	Malicious File Transfer - UNC5487, REMCOS, SHADOWLADDER, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,Malware:SHADOWLADDER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-031	Malicious File Transfer - UNC5487, REMCOS, SHADOWLADDER, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,Malware:SHADOWLADDER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-032	Malicious File Transfer - UNC5487, REMCOS, SHADOWLADDER, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,Malware:SHADOWLADDER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-033	Malicious File Transfer - UNC5487, REMCOS, SHADOWLADDER, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,Malware:SHADOWLADDER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-034	Malicious File Transfer - UNC5487, REMCOS, SHADOWLADDER, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,Malware:SHADOWLADDER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-035	Malicious File Transfer - UNC5487, REMCOS, SHADOWLADDER, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,Malware:SHADOWLADDER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-036	Malicious File Transfer - UNC5487, REMCOS, SHADOWLADDER, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,Malware:SHADOWLADDER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-037	Malicious File Transfer - UNC5487, REMCOS, SHADOWLADDER, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,Malware:SHADOWLADDER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-038	Malicious File Transfer - UNC5487, REMCOS, SHADOWLADDER, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,Malware:SHADOWLADDER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-039	Malicious File Transfer - UNC5487, REMCOS, SHADOWLADDER, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,Malware:SHADOWLADDER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-040	Malicious File Transfer - UNC5487, REMCOS, SHADOWLADDER, SHADOWLADDER.IDAT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5487,CAMP.25.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:REMCOS,Malware:SHADOWLADDER,Malware:SHADOWLADDER.IDAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-041	Malicious File Transfer - UNC5669, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-042	Malicious File Transfer - UNC5669, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-043	Malicious File Transfer - UNC5669, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-044	Malicious File Transfer - UNC5669, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-045	Malicious File Transfer - UNC5669, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-046	Malicious File Transfer - UNC5669, Download, Variant #15	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-047	Malicious File Transfer - UNC5669, Download, Variant #16	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-048	Malicious File Transfer - UNC5669, Download, Variant #17	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-049	Malicious File Transfer - UNC5669, Download, Variant #18	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-050	Malicious File Transfer - UNC5669, Download, Variant #19	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,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
A109-051	Malicious File Transfer - UNC5669, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-052	Malicious File Transfer - UNC5669, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-053	Malicious File Transfer - UNC5669, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-054	Malicious File Transfer - UNC5669, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-055	Malicious File Transfer - UNC5669, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-056	Malicious File Transfer - UNC5669, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-057	Malicious File Transfer - UNC5669, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-058	Malicious File Transfer - UNC5669, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-059	Malicious File Transfer - UNC5669, XWORM, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5669,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:XWORM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-060	Malicious File Transfer - UNC5795, AEROSTAT, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,CAMP.26.071,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:AEROSTAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-061	Malicious File Transfer - UNC5795, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,CAMP.26.071,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-062	Malicious File Transfer - UNC5795, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,CAMP.26.071,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-063	Malicious File Transfer - UNC5795, HOTAIR, Download, Variant #14	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5795,CAMP.26.071,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTAIR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-064	Malicious File Transfer - UNC6240, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6240,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-065	Malicious File Transfer - UNC6240, MESHAGENT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6240,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MESHAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-066	Malicious File Transfer - UNC6240, MESHAGENT, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6240,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MESHAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-067	Malicious File Transfer - UNC6240, MESHAGENT, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6240,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MESHAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-068	Malicious File Transfer - UNC6279, VEILDRIVE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6279,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VEILDRIVE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-069	Malicious File Transfer - UNC6492, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6492,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
A109-070	Malicious File Transfer - UNC6492, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6492,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-071	Malicious File Transfer - UNC6527, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6527,CAMP.25.076,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-072	Malicious File Transfer - UNC6527, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6527,CAMP.25.076,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-073	Malicious File Transfer - UNC6527, FLUXWEAVE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6527,CAMP.25.076,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FLUXWEAVE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-074	Malicious File Transfer - UNC6527, FLUXWEAVE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6527,CAMP.25.076,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FLUXWEAVE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-075	Malicious File Transfer - UNC6534, BADTILE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6534,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-076	Malicious File Transfer - UNC6534, BADTILE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6534,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-077	Malicious File Transfer - UNC6534, BADTILE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6534,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-078	Malicious File Transfer - UNC6633, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6633,CAMP.26.075,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
A109-079	Malicious File Transfer - UNC6633, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6633,CAMP.26.075,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-080	Malicious File Transfer - UNC6633, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6633,CAMP.26.075,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-081	Malicious File Transfer - UNC6633, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6633,CAMP.26.075,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-082	Malicious File Transfer - UNC6633, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6633,CAMP.26.075,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-083	Malicious File Transfer - UNC6633, JADECLIP, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6633,CAMP.26.075,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:JADECLIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-084	Malicious File Transfer - UNC6633, JADECLIP, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6633,CAMP.26.075,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:JADECLIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-085	Malicious File Transfer - UNC6699, BADTILE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6699,CAMP.26.063,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-086	Malicious File Transfer - UNC6699, BADTILE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6699,CAMP.26.063,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-087	Malicious File Transfer - UNC6699, BADTILE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6699,CAMP.26.063,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-088	Malicious File Transfer - UNC6699, BADTILE, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6699,CAMP.26.063,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-089	Malicious File Transfer - UNC6699, BADTILE, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6699,CAMP.26.063,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-090	Malicious File Transfer - UNC6699, BADTILE, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6699,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-091	Malicious File Transfer - UNC6699, BADTILE, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6699,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-092	Malicious File Transfer - UNC6699, BADTILE, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6699,CAMP.26.063,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-093	Malicious File Transfer - UNC6699, BADTILE, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6699,CAMP.26.063,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BADTILE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-094	Malicious File Transfer - UNC6727, SUNBRICKED, 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,Malware:SUNBRICKED,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-095	Malicious File Transfer - UNC6780, FIRESCALE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,CAMP.26.060,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FIRESCALE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-096	Malicious File Transfer - UNC6780, FIRESCALE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,CAMP.26.060,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FIRESCALE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-097	Malicious File Transfer - UNC6780, RAMENRUMBLE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6780,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:RAMENRUMBLE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-098	Malicious File Transfer - UNC6828, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6828,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-099	Malicious File Transfer - UNC6828, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6828,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-100	Malicious File Transfer - UNC6828, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6828,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-101	Malicious File Transfer - UNC6828, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6828,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-102	Malicious File Transfer - UNC6828, MELTRUBY, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6828,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MELTRUBY,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-103	Malicious File Transfer - UNC6836, SOMBERMEME, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6836,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SOMBERMEME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-104	Malicious File Transfer - UNC6836, SOMBERMEME, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6836,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SOMBERMEME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-105	Malicious File Transfer - UNC6836, SOMBERMEME, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6836,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SOMBERMEME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-106	Malicious File Transfer - UNC6836, SOMBERMEME, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6836,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SOMBERMEME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-107	Malicious File Transfer - UNC6836, SOMBERMEME, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6836,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SOMBERMEME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-108	Malicious File Transfer - UNC6836, SOMBERMEME, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6836,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SOMBERMEME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-109	Malicious File Transfer - UNC6849, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6849,CAMP.26.059,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-110	Malicious File Transfer - UNC6849, NEONSLIDE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6849,CAMP.26.059,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NEONSLIDE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-111	Malicious File Transfer - UNC6849, VIDAR, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6849,CAMP.26.059,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VIDAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-112	Malicious File Transfer - UNC6849, VIDAR, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6849,CAMP.26.059,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:VIDAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-113	Malicious File Transfer - UNC6863, SLICKDEMON, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6863,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-114	Malicious File Transfer - UNC6863, SLICKDEMON, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6863,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-115	Malicious File Transfer - UNC6863, SLICKDEMON, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6863,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-116	Malicious File Transfer - UNC6863, SLICKDEMON, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6863,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-117	Malicious File Transfer - UNC6863, SLICKDEMON, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6863,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-118	Malicious File Transfer - UNC6863, SLICKDEMON, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6863,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-119	Malicious File Transfer - UNC6863, SLICKDEMON, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6863,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-120	Malicious File Transfer - UNC6863, SLICKDEMON, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6863,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLICKDEMON,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-121	Malicious File Transfer - UNC6868, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6868,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-122	Malicious File Transfer - UNC6876, HEAVYMETAL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6876,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HEAVYMETAL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-123	Malicious File Transfer - UNC6876, HEAVYMETAL, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6876,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HEAVYMETAL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-124	Malicious File Transfer - UNC6923, 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,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-125	Malicious File Transfer - UNC6923, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6923,CAMP.26.080,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-126	Malicious File Transfer - UNC6923, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6923,CAMP.26.080,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-127	Phishing Email - Malicious Attachment, UNC5795, HOTAIR, Variant #2	ATT&CK:Initial Access,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:M1049,ATT&CK:M1054,ATT&CK:T1566.001,Actor:UNC5795,Control:Email,Malware:HOTAIR,NIST:CM-7,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted

New Files

A total of 329 new files have been added to the File Library with this update. This includes 329 malicious files.

Malicious Files

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
03a59ea3d8e78ffaf5acd11be39d94d3	Malware:SHUBSTAKE,Malware_Type:DATA_MINER,Group:Validation
04750aba368eeb2890e74d10fa0a50a3	Malware:FIRESCALE,Group:Validation
0531048e9e0e34f29f551dd985d4b458	Malware:FAKEUPDATES,Malware_Type:DOWNLOADER,Group:Validation
0599ef077bc089475153a8cf2ffa9695	Malware:CYANSPEAR,Group:Validation
05de94a0d6666fe89c8af033070b2133	Malware_Type:DROPPER_MEMORY_ONLY,Malware:COILCAGE,Group:Validation
07df1be05e8d7e6f4e9c738f8544054e	Malware:BLUEBEAM.ASP,Group:Validation
07f74b7d16181dec1401c85f8ebe45f3	Malware:MELTRUBY,Malware_Type:BACKDOOR,Group:Validation
0a487dcd6ef8f98d7fcee0583592a89b	Malware:SANDCLOCK,Group:Validation
0a557a7c308935af2d948fae75f10537	Malware_Type:DATA_MINER,Group:Validation,Malware:SHUBSTAKE
0ba348cdebc00bc157a7c8e3fa018cfe	Group:Validation,Malware:KAITEN
0bb6384f0eae9335036a2233692e71e5	Malware:DUSTMAKER,Group:Validation
0bbb31fab91d223055407617afbca3db	Malware:HEAVYMETAL,Malware_Type:BACKDOOR,Group:Validation
0d07810f455e7bd0915303db96351f3c	Group:Validation,Malware:BADTILE,Malware_Type:BACKDOOR
0d34b7d8aee1f6e18430947551896fa3	Malware_Type:DOWNLOADER,Malware:FAKEUPDATES,Group:Validation
0da0cfa64a73418bc167f24c1aa8ab17	Malware_Type:BACKDOOR,Malware:REDSONJA.KINSING,Group:Validation
0e6a23c23b379a7587d6855fb8be4afd	Malware:EFSPOTATO,Group:Validation
0e9f8fdc5d3124d2b6fad948446849b4	Group:Validation,Malware:COILCAGE,Malware_Type:DROPPER_MEMORY_ONLY
0fdcc01f577c847a9ab98ffbf63a9c69	Malware_Type:BACKDOOR,Malware:REDSONJA.KINSING,Group:Validation
1004a0df8dd34741b40ed6bc3c04ade5	Malware_Type:BACKDOOR,Malware:ENSYNCROLL,Group:Validation
107407bcb9f32fa97ad0e598aaa67a2a	Malware_Type:BACKDOOR,Malware:JADECLIP,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
11e29fe2df34e658e1727303aaf8e728	Malware:SHUBSTAKE,Malware_Type:DATA_MINER,Group:Validation
11fe813d88e5b293fbeccc77b10689cc	Group:Validation,Malware:KAITEN
121e720aaa707daaf7d88df547750762	Malware_Type:DOWNLOADER,Group:Validation,Malware:FAKEUPDATES
1393e730850e5cb9cf6f182bd1e41fe3	Malware:REMCOS,Group:Validation,Malware_Type:BACKDOOR
13b8bb087f043eb3058829180499f28f	Group:Validation,Malware:SLICKDEMON,Malware_Type:DATA_MINER
13d81c56870be29e204e4325664f2b26	Group:Validation
147c5068a8135a5f066cb469e6aa828a	Malware_Type:DATA_MINER,Malware:SHUBSTAKE,Group:Validation
14885b8b198bda3225e631169931eb6a	Malware:EFSPOTATO,Group:Validation
16dbffd3f1e14f9dfada7bc5fbaba3b1	Malware:CURLYGATE,Group:Validation,Malware_Type:DOWNLOADER
173e4b2a8374f1798ce24fc12c3f7859	Malware_Type:DOWNLOADER,Group:Validation,Malware:FAKEUPDATES
178675155af850d5deca6773709ac9fb	Malware:BADTILE,Malware_Type:BACKDOOR,Group:Validation
19b9606190658ffa682423a7fc19f994	Malware_Type:BACKDOOR,Malware:REMCOS,Group:Validation
1a0513684ba454e351594e8ab4fd87c2	Malware_Type:DOWNLOADER,Group:Validation,Malware:FAKEUPDATES
1b7cc1d4161a290f1a96050dbfb56a41	Malware_Type:BACKDOOR,Malware:MASOL,Group:Validation
1cb65dce1f1b58710cc9b630ccc51fc8	Malware_Type:DOWNLOADER,Malware:LONGWAIT,Group:Validation
1cbe60054bcb4e9aca46d11dd1890e6c	Malware_Type:DATA_MINER,Malware:SLICKDEMON,Group:Validation
1d6184202d8b09c2990efd5e063073fb	Malware_Type:DOWNLOADER,Malware:NEONSLIDE,Group:Validation
1d98761695b2d33a7be5305a10f3f67a	Malware:DUSTMAKER,Group:Validation
1fafb0565b216c5dc74e1aabb645d8fb	Malware:CYANSPEAR,Group:Validation
1fe02eb6921f7dc6907fabce3cefe4c2	Malware_Type:BACKDOOR,Malware:REMCOS,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
200f59f60e4585689c540f9940621978	Malware:CURLYGATE,Malware_Type:DOWNLOADER,Group:Validation
2081c91d1bc001ffdaf1d1a83cdd72ed	Group:Validation
24af59fbf7e8895487506b0cc2f372fb	Malware:FAKEUPDATES,Group:Validation,Malware_Type:DOWNLOADER
26a714fd92758876160306721 01efda2	Malware_Type:BACKDOOR,Malware:REDSONJA.KINSING,Group:Validation
26b065e33822889274af439cc7f7eb25	Group:Validation
28836bd9d84b189f3c6fad56b80254df	Malware:NEONSLIDE,Malware_Type:DOWNLOADER,Group:Validation
288f86176636f6d39bc16186e4c45bc5	Malware:KAITEN,Group:Validation
292e142e7a8e3ddbb067fa151e472aba	Malware:SHUBSTAKE,Malware_Type:DATA_MINER,Group:Validation
296203c4ce5c32d82f406b96c09c82b4	Malware:SLICKDEMON,Malware_Type:DATA_MINER,Group:Validation
2ab34636eeab843b4bcbb6e44f033eab	Malware_Type:INSTALLER,Malware:HOTAIR,Group:Validation
2b0be4e5c3a3a54a4dd04e2bb536ce66	Group:Validation
2beb2e15570aac6370935bf76543e9fd	Malware:SHUBSTAKE,Malware_Type:DATA_MINER,Group:Validation
2cb3ac34d6c469d543fc9cb24ba0e860	Malware:FLUXWEAVE,Malware_Type:DOWNLOADER,Group:Validation
2d3e76e0d2c7df078efe47e03fbc4f50	Group:Validation
2db7d9b12aee112abc4730dd2d601776	Group:Validation,Malware:CURLYGATE,Malware_Type:DOWNLOADER
2ef9ee28ca5387a71ed1bd528bf6c260	Malware_Type:TUNNELER,Malware:VIPERTUNNEL,Group:Validation
2f1eab4755372383641d87351a215a6b	Group:Validation,Malware:COILCAGE,Malware_Type:DROPPER_MEMORY_ONLY
329f0dd70c28274a5b64982a44211622	Malware_Type:BACKDOOR,Malware:REMCOS,Group:Validation
32bf6553da4658348f81afca04a24056	Group:Validation
3318c614fa7d74b71c81f0e5532cc27e	Malware_Type:BACKDOOR,Group:Validation,Malware:SOMBERMEME

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
34af888f33898a4c3b93ac0e8fecf3a2	Malware_Type:BACKDOOR,Malware:ENSYNCROLL,Group:Validation
35365d5022418c313386d1f0dcc365e9	Group:Validation
3681713dd67af8bfe7c624e5d5a16db7	Malware:BLUEBEAM.PHP,Group:Validation
36c697881561026c941ff7594077f564	Malware:SLICKDEMON,Malware_Type:DATA_MINER,Group:Validation
3704b400b2fa09935d59b6d3349c06d9	Malware_Type:BACKDOOR,Malware:REMCOS,Malware:SHADOWLADDER,Group:Validation
3712793d3847dd0962361aa528fa124c	Malware:SUGARLOADER,Group:Validation,Malware_Type:DOWNLOADER
3818f4bd242cf6b910c70ad55ef3e9c4	Malware:KAITEN,Group:Validation
386b6379cf1cea09b2fe8e69432f8c9f	Group:Validation
3932ba3bcd7854a1fa3dce4bbd35ccc4	Group:Validation,Malware_Type:DOWNLOADER,Malware:CURLYGATE
39412f55f3db7c60274f4671bf8b4fe4	Malware_Type:BACKDOOR,Malware:JADECLIP,Group:Validation
398de7b83f0fe06c17b1c8ee56d0d5a6	Malware:SLICKDEMON,Malware_Type:DATA_MINER,Group:Validation
3a36a7a42b6df7951494a84983ac3500	Malware:REMCOS,Group:Validation,Malware_Type:BACKDOOR
3a4aa939c18f3e0ac0417c48e3fa977c	Malware:DUSTMAKER,Group:Validation
3a6b966440fa704a6d6066590f5842c1	Malware_Type:BACKDOOR,Malware:SHADOWLADDER,Malware:REMCOS,Group:Validation
3b2d72060481181300cf8c676e8ceef0	Malware:SHUBSTAKE,Malware_Type:DATA_MINER,Group:Validation
3b967be216053c7722a5e32eca70ea2c	Malware:SHADOWLADDER.IDAT,Malware:REMCOS,Group:Validation,Malware_Type:DROPPER
3b98155e3425749bb202c9993d3e03e6	Malware:SHUBSTAKE,Malware_Type:DATA_MINER,Group:Validation
3bd31a1d91c9a7db89c17874ce0c3447	Group:Validation
3d7d58ee24ac41be838b707d666d227e	Group:Validation,Malware:SHUBSTAKE,Malware_Type:DATA_MINER
3e506529f1008d7a1ff20e488baf32f0	Malware_Type:DOWNLOADER,Group:Validation,Malware:OAKSHADE

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
40977c4e1633548553c79a8d73b4e830	Malware_Type:BACKDOOR,Malware:RAMENRUMBLE,Group:Validation
41016a6fa4f83d49383c1e7896859761	Malware_Type:BACKDOOR,Malware:MELTRUBY,Group:Validation
4186a9a9de2fdce249f4731ad63d0ed3	Malware:BADTILE,Malware_Type:BACKDOOR,Group:Validation
432a1864c149888282eebcd3650a8363	Malware_Type:DOWNLOADER,Group:Validation
433902681dd4579d5e3ece5df17e0607	Malware:REMCOS,Malware_Type:BACKDOOR,Malware:SHADOWLADDER,Group:Validation
4495b10eed13887ded1fecc4041792ab	Malware_Type:BACKDOOR,Malware:REMCOS,Group:Validation
4562923b409b77af995eff080bf37552	Group:Validation,Malware:BLUEBEAM.PHP
46655af59b65a882bd742ba1934c8a5f	Malware_Type:DOWNLOADER,Malware:FAKEUPDATES,Group:Validation
4821b7942df952a65a9ae6514303470c	Malware:DUSTMAKER,Group:Validation
482cc72e01dfa54f30efe4fefde5422d	Malware_Type:BACKDOOR,Malware:BADTILE,Group:Validation
49b931da0e3bf0a40348ad603c674846	Group:Validation,Malware:CYANSPEAR
49ebcb5090c8eb83059ed5b864715447	Group:Validation
4cb6fd2e9a585a7b1b57a07cd86ff2d9	Group:Validation,Malware_Type:DATA_MINER,Malware:SLICKDEMON
4eac47c18e78c4e107298e165009ef4e	Malware_Type:DROPPER_MEMORY_ONLY,Malware:SYSTEMBC.V2,Group:Validation
4f02130a230dabdbe6b8591e17060422	Malware:MELTRUBY,Group:Validation,Malware_Type:BACKDOOR
5011bf6b70c6b6c91e410568c267c8e2	Malware_Type:BACKDOOR,Malware:REMCOS,Group:Validation
51203b06eddd7c21d313b23e143c1bc3	Group:Validation
52081dfba55ec58dc83c982f88c696f4	Group:Validation,Malware:BADTILE,Malware_Type:LAUNCHER
52e0dc4e4e2fa234bd7a6ac54b899643	Group:Validation
5343acec6ef763a87c105ccf426228ac	Malware_Type:BACKDOOR,Malware:REMCOS,Group:Validation,Malware:SHADOWLADDER
53c2a6cc026c855253d816464b14deb7	Group:Validation,Malware:KAITEN

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
544f2df417673c546f9a2ccb13cef87f	Malware_Type:DOWNLOADER,Malware:NEONSLIDE,Group:Validation
5455e769b16ea790c80c1fc9a443540e	Malware:COILCAGE,Group:Validation,Malware_Type:DROPPER_MEMORY_ONLY
56304316dca1b589cf75263d1bb1e592	Malware_Type:LAUNCHER,Malware:BADTILE,Group:Validation
56e21d8ab319f55d34146e45609858d2	Malware:SHUBSTAKE,Group:Validation,Malware_Type:DATA_MINER
58ac2f65e335922be3f60e57099dc8a3	Group:Validation
58ee8cf9fd2546c9a56d6b59471fb743	Malware:SYSTEMBC.V2,Malware_Type:TUNNELER,Group:Validation
59b2e032fb8a73a17dd24664bba31f06	Group:Validation,Malware:EFSPOTATO
5a4c6568941e638f26f57f610a2a5d3b	Group:Validation
5aa168e5e2df972ae767531667c03b52	Group:Validation,Malware:DUSTMAKER
5c1f1afbe37b5a17e89536afa7651c98	Malware:FLUXWEAVE,Malware_Type:DOWNLOADER,Group:Validation
5c72a3cd9984837379a1b7fbb1496cde	Group:Validation
5dee6e306df05f1d15dc4089251f9cbd	Malware_Type:DOWNLOADER,Group:Validation
5dfcd09d6c7b6c334ff47e302fb305f4	Group:Validation,Malware_Type:BACKDOOR
5e5556c1bc7c69b64027845dd184bf09	Malware_Type:DOWNLOADER,Group:Validation,Malware:CURLYGATE
5ec744012ed51dad33831a44cede11da	Malware:SLICKDEMON,Malware_Type:DATA_MINER,Group:Validation
5f6dc8f19140bba5086dba996127754d	Group:Validation,Malware_Type:BACKDOOR
609bde3e3c85c6f79a9ec5fdd1ed6de7	Malware:NEONSLIDE,Group:Validation,Malware_Type:DOWNLOADER
60b9584e576003bc4a9b7a6f6a1a5c19	Malware:MELTRUBY,Malware_Type:BACKDOOR,Group:Validation
60c7ee212025d63fb725c36e004cf7fd	Malware_Type:BACKDOOR,Malware:REMCOS,Group:Validation
60ff7811088e50919759af00ad9b168f	Malware:CURLYGATE,Group:Validation,Malware_Type:DOWNLOADER
616a75cb68ff2b784d4b81385a485b4f	Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
639e8ee77d71f01d7ecd78ecc1727a06	Group:Validation,Malware:DUSTMAKER
63a18b8f208311e181444ecd92ddd6fd	Malware:CURLYGATE,Malware_Type:DOWNLOADER,Group:Validation
63cf5d19607df2bcefc84647021944c4	Malware_Type:DOWNLOADER,Malware:CURLYGATE,Group:Validation
63d839d7ed05876a80dbedc6a040c34b	Group:Validation,Malware:CYANSPEAR
645b0bae647c40ba173cd44f841ddca0	Group:Validation
666ba36c5e1a3c4ea2bcbb94cf56c070	Malware:DUSTMAKER,Group:Validation
6855dedfe19b2169eb2fd554b9d6ef6e	Malware_Type:BACKDOOR,Group:Validation,Malware:REMCOS,Malware:SHADOWLADDER
6970be88e339eded36cc7cb7fcadaa6b	Malware_Type:BACKDOOR,Malware:REMCOS,Group:Validation,Malware:SHADOWLADDER
6b9e33443c2d6427acb8fab60d6541ca	Malware_Type:DOWNLOADER,Group:Validation,Malware:FAKEUPDATES
6bdc59715888cf8004616da6090464b3	Malware_Type:DOWNLOADER,Malware:NEONSLIDE,Group:Validation
6e47397c21cf41c29d6f7472a4c0162f	Malware:DUSTMAKER,Group:Validation
6e95d4728c5b2b4dc2ee46598c9d0e01	Malware:BADTILE,Malware_Type:BACKDOOR,Group:Validation
6f4404dad0b9409e92e0996f860a9a19	Malware_Type:BACKDOOR,Malware:SHADOWLADDER,Malware:REMCOS,Group:Validation
6f48f21ee548b385cc0c65cb9070a580	Malware:BADTILE,Malware_Type:BACKDOOR,Group:Validation
701b82631ccb33685b758011651bdbef	Malware:EFSPOTATO,Group:Validation
70429067e63b17cee245c438ab9129ed	Malware_Type:DOWNLOADER,Malware:FAKEUPDATES,Group:Validation
7244a27029d2fb104a598b40e9f284d9	Malware:AEROSTAT,Group:Validation
73ad90ff79c8c94d99f93698b99891ab	Malware_Type:DOWNLOADER,Group:Validation
7527326a84bcf8501cc54210497386fd	Malware:BLUEBEAM.PHP,Group:Validation
7530e3db4e117eb623e44ac9f8820d53	Malware:MELTRUBY,Malware_Type:BACKDOOR,Group:Validation
767152e96a401b8c48487a559d0bd242	Group:Validation,Malware:EFSPOTATO

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
7710dc4fdde666bd1d6d097d38d6c0e5	Malware_Type:DOWNLOADER,Group:Validation,Malware:CURLYGATE
792df5729adac6ee3120d97b30ccfee8	Malware:FAKEUPDATES,Group:Validation,Malware_Type:DOWNLOADER
7bd3201946ef8b8a836bc2f951923adc	Malware_Type:BACKDOOR,Malware:SOMBERMEME,Group:Validation
7e22fd1d2517ca81ea8338c958878bff	Malware_Type:DOWNLOADER,Malware:CURLYGATE,Group:Validation
7eeee2fb2390aa5eafc5b24c17a9db94	Malware_Type:DATA_MINER,Group:Validation,Malware:SLICKDEMON
7f061e76dde1bdd21b58b07463964579	Malware:FAKEUPDATES,Malware_Type:DOWNLOADER,Group:Validation
7f409ef4ecc50db598bc1dc4afff8250	Malware_Type:TUNNELER,Group:Validation,Malware:VIPERTUNNEL
806af3f5ad3db5fa23d46292e4dd702b	Malware:EFSPOTATO,Group:Validation
8143f27e3e6efb40042d4abcb1f8e257	Malware:KAITEN,Group:Validation
833368e3029a38a4f87207acd537070e	Group:Validation
83d3f32cfbbaa13a3eace9dd0b8d9dd4	Malware:DUSTMAKER,Group:Validation
84e9bbaf802be04ae4c4ae46b034d7d2	Malware_Type:BACKDOOR,Malware:MATANBUCHUS,Group:Validation
860ef29773cf680ed765cb08ac3072cb	Group:Validation,Malware_Type:BACKDOOR,Malware:SOMBERMEME
863c576f70be9dd7a5d817f4dcd0323f	Malware:SOMBERMEME,Group:Validation,Malware_Type:BACKDOOR
86c9eb0bce08c317b83b466e17e25235	Group:Validation,Malware:EFSPOTATO
86da7ba7ed03fdc6950f1d1ec9923a49	Malware:SANDCLOCK,Group:Validation
8771c1b08ad959dc2162131eacfbcea3	Group:Validation,Malware:DUSTMAKER
87c75c0df3e1c32e64d4c9ea129fcff9	Malware:MESHAGENT,Group:Validation
88da420dd5d82f1ca7c247f1305e37c4	Malware:CYANSPEAR,Group:Validation
89658d3986921a5001cf59882cccf539	Malware_Type:DOWNLOADER,Malware:FAKEUPDATES,Group:Validation
8a7209048607f42700a751b6afac72fa	Group:Validation,Malware:SHUBSTAKE,Malware_Type:DATA_MINER

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
8aa6e7020764f9f818e2cbec77964882	Group:Validation,Malware:KAITEN
8acbbd48ebbd74af10d0ad8b11f11c20	Group:Validation,Malware:KAITEN
8b79f38187b715e556d88b01233757fb	Malware_Type:BACKDOOR,Malware:REDSONJA.KINSING,Group:Validation
8c39ed598b740214564a2cbeb43601df	Group:Validation,Malware_Type:DATA_MINER,Malware:SLICKDEMON
8c561e80d3333d183ac8157bae44e3bd	Malware:VIPERTUNNEL,Malware_Type:TUNNELER,Group:Validation
8d76423d72e1349deccf52b6c68ca3dd	Malware:EFSPOTATO,Group:Validation
8dc0ccbe0392c932f7bac35e6bbd6160	Malware:MATANBUCHUS,Malware_Type:BACKDOOR,Group:Validation
8ea5693c170609f0e0305f940ff6a0fe	Malware:CURLYGATE,Malware_Type:DOWNLOADER,Group:Validation
8eba223ff475f4788c5b7cdae7021515	Malware_Type:BACKDOOR,Malware:REMCOS,Group:Validation
8ecb24b4bf862c512ed6df86eeaed0f4	Group:Validation
8f0e1e2b6049aecb2ffe377d7505e3bd	Malware_Type:BACKDOOR,Malware:VEILDRIVE,Group:Validation
8f60d0ce1aecdbcf0de2800380584d65	Malware:BADTILE,Malware_Type:BACKDOOR,Group:Validation
8f6cec6f5436eb0fe79a1f26a1c663d4	Malware_Type:DOWNLOADER,Malware:SUNBRICKED,Group:Validation
9206d315aa8a5372d4096ef9858dd0eb	Group:Validation,Malware_Type:DATA_MINER,Malware:SHUBSTAKE
9215b38ac9e301840186e0405679b990	Malware:CURLYGATE,Malware_Type:DOWNLOADER,Group:Validation
92d4c251d01f1f8f907ba71942c2dca5	Malware_Type:DOWNLOADER,Group:Validation,Malware:CURLYGATE
93119da3116b60fd1718627f51a5c11a	Malware:SHUBSTAKE,Group:Validation,Malware_Type:DATA_MINER
93161aa146583dffe34dde804decfdb7	Malware:VIDAR,Malware_Type:DATA_MINER,Group:Validation
9330667df5ebbcaea64bb9d3fa824046	Malware_Type:LAUNCHER,Malware:JADECLIP,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
947a7cf1fc493d1060c1289c35bed764	Malware_Type:BACKDOOR,Malware:REMCOS,Group:Validation,Malware:SHADOWLADDER
94d967b7d394a022daacba4de35d9bbd	Malware_Type:DROPPER_MEMORY_ONLY,Malware:COILCAGE,Group:Validation
95d4840d4c5c434126f47f4eb7621730	Malware:DUSTMAKER,Group:Validation
95e713201d3142296457ed202816e5a0	Malware_Type:BACKDOOR,Malware:REMCOS,Group:Validation
95f31259fbe96d9265ef3d71ad63f1d1	Malware:CURLYGATE,Malware_Type:DOWNLOADER,Group:Validation
974eb3d5bd550feaea763f6d7f3f2b97	Group:Validation
97f341e081cd0323fb9ea055a237496d	Malware:REMCOS,Malware_Type:BACKDOOR,Group:Validation
9806255b07cd6793bb33682f53eb499a	Malware_Type:BACKDOOR,Malware:BADTILE,Group:Validation
985a4489738b8dd62f66179151717ba1	Malware:BLUEBEAM.ASP,Group:Validation
98eea8d9c81ba3fa704ce44918b81dbb	Malware_Type:DOWNLOADER,Malware:FAKEUPDATES,Group:Validation
98f9101bdd25da3a54da1891ae57f3dc	Malware_Type:BACKDOOR,Malware:SOMBERMEME,Group:Validation
998d0cef86ea34fce7281631ddd2bc06	Malware_Type:BACKDOOR,Malware:REMCOS,Group:Validation
9bb1cc315675e1a41492ef2d52ac160d	Malware_Type:DATA_MINER,Malware:SLICKDEMON,Group:Validation
9bce75300b367a8cad32ff6ed88752a1	Malware_Type:DOWNLOADER,Malware:NEONSLIDE,Group:Validation
9cbb03932dc71ca41c418d020b10b5ff	Malware_Type:DATA_MINER,Malware:SLICKDEMON,Group:Validation
9d1bb4d2bc0874fe839f826bdf0956a6	Malware:DUSTMAKER,Group:Validation
9e4d424f53eae382f1f736ca611421b5	Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation,Malware:VIPERTUNNEL,Malware:COILCAGE
9ebcd560c2bd3ec5fe56e488e5a4f546	Group:Validation,Malware:BADTILE,Malware_Type:BACKDOOR
9f4a085f129c06efbd06b3889a3eabf5	Group:Validation
9f5c71d16c2aaa8023088d65b748791e	Malware:EFSPOTATO,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
a004a3a617b40ebb55799186f9c01a86	Malware_Type:BACKDOOR,Malware:SHADOWLADDER,Malware:REMCOS,Group:Validation
a12957e7627cb19fba2a4b155f7258b7	Group:Validation
a188e095f91e0963b797e1ff8582ed79	Malware_Type:DOWNLOADER,Group:Validation
a4722148cc21fd279ab441360e5d068b	Group:Validation
a4da845577dad59877eccfd1839971ae	Malware_Type:DATA_MINER,Group:Validation,Malware:SHUBSTAKE
a54761cc3e2f11a97eec4a2b658b5edf	Malware:EFSPOTATO,Group:Validation
a577ed807b42198ae3634bce83954c1e	Group:Validation
a5ddc4a3c44308332ed885ca52ead588	Group:Validation,Malware:LONGWAIT,Malware_Type:DOWNLOADER
a5ef4130e1c6514312ece0d9bd9054d4	Malware_Type:DOWNLOADER,Malware:CURLYGATE,Group:Validation
a6513d76588d451673e5754f61c85055	Malware:BLUEBEAM.JSP,Group:Validation
a71949ece5b7518880e4681425a72fe0	Malware:BLUEBEAM.PHP,Group:Validation
a7b63611c465709759e01a5966bc80fb	Malware_Type:BACKDOOR,Malware:MASOL,Group:Validation
a7d495ec807ac57658df4a86e8c38fc9	Group:Validation,Malware:KAITEN
a97583eb4dfd1673a6c511e40f23f7ad	Malware:CURLYGATE,Malware_Type:DOWNLOADER,Group:Validation
aaaccca9cbd235e28414ba57523db5a0	Malware:SHUBSTAKE,Group:Validation,Malware_Type:DATA_MINER
ab2a0322fd0d3616a0f262fc5958d033	Group:Validation,Malware:SANDCLOCK
ab68baf963eaaec4aa7a0d2308b18846	Malware_Type:BACKDOOR,Malware:REDSONJA.KINSING,Group:Validation
ac572439fffca0e988c14c351a42668e	Malware:EFSPOTATO,Group:Validation
ac9ce47289e0f86e6be4c2c184ac9d94	Malware:BADTILE,Malware_Type:BACKDOOR,Group:Validation
acf6a9018af01c9ff9f862726ad77736	Group:Validation,Malware:BLUEBEAM.JSP
ade31ddb613b181f95ca43b317bd7b15	Malware:NEONSLIDE,Malware_Type:DOWNLOADER,Group:Validation
afe95ec1e2e9606387ce6679e6d77ee2	Malware:PLAYCRYPT,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
b06b126b9e26af03a7ef2f8b8e90d446	Malware_Type:BACKDOOR,Malware:RAMENRUMBLE,Group:Validation
b11a31ef6947c9b067b1a91f962219d6	Malware_Type:BACKDOOR,Malware:REDSONJA.KINSING,Group:Validation
b1b70fc031faaca17a2d9e5486b2e5ba	Malware:PEATWIRE,Group:Validation
b228cb94ee99e1fcd0b2cac5320e06e0	Malware_Type:BACKDOOR,Malware:MELTRUBY,Group:Validation
b53f5d8baf6840fa3a5ea8e56d208ddf	Group:Validation
b61100942e2d65a90fc7c4d69b83da74	Malware:CYANSPEAR,Group:Validation
b7161246c3e4926349602c66d65a528f	Group:Validation
b75df073648061ec28a456f5a699d257	Malware:KAITEN,Group:Validation
b7af1868d3c5838c30d7d90521c7a721	Malware:MESHAGENT,Group:Validation
ba78c9581e8b48a1632e3de854fbf985	Group:Validation
bb02266d74190c5a8f523c84b58f0d49	Malware:BADTILE,Malware_Type:BACKDOOR,Group:Validation
bbfd599a76a6420cf1a77f5cf27046b7	Malware_Type:DOWNLOADER,Group:Validation,Malware:FAKEUPDATES
bd29b868e6594efead8665e575e4c73c	Malware_Type:BACKDOOR,Malware:MELTRUBY,Group:Validation
c17f39d25def01d5c87615388925f45a	Malware_Type:BACKDOOR,Malware:BADTILE,Group:Validation
c1972bae94d24e7a5daafbcfe030fd8d	Group:Validation
c1b9834997f30d5ec572b91e844a9615	Malware_Type:DATA_MINER,Malware:SHUBSTAKE,Group:Validation
c1e4857fee9b303f4b80d9b13456ab91	Group:Validation,Malware:KAITEN
c1e8e8cfc18f08e0f3c0f93d2ff98966	Malware:EFSPOTATO,Group:Validation
c21e09fd60f812fd7008ba03ee1e4557	Malware_Type:BACKDOOR,Malware:BADTILE,Group:Validation
c2f7fd326c38cc591d575cbb84373b7c	Malware_Type:BACKDOOR,Malware:BADTILE,Group:Validation
c2fec2e8c00dc5b2dfbce212d5b75188	Malware_Type:DOWNLOADER,Malware:FAKEUPDATES,Group:Validation
c353111816e5da87ace854f1b3a7aa7e	Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
c372587a627f5f915aff74fb805d4423	Malware:BADTILE,Malware_Type:BACKDOOR,Group:Validation
c4341b5fb3dd998e17db4c5e18ae03d4	Malware_Type:DOWNLOADER,Group:Validation
c650a624455c5222906b60aac7e57d48	Malware_Type:LAUNCHER,Malware:BADTILE,Group:Validation
c6e2258d994094421dcabd00b47e5f2c	Malware_Type:DOWNLOADER,Malware:NEONSLIDE,Group:Validation
c6e2f42f9780190b86eed411931485c5	Malware_Type:BACKDOOR,Malware:SHADOWLADDER,Malware:REMCOS,Group:Validation
ca542e26771fde2957fccf09d7471089	Malware:EFSPOTATO,Group:Validation
cb22e73b588ef4f540308285324d3fee	Group:Validation
cb25f0cdb88e25bd7a5acb4c0ce671c5	Malware_Type:DOWNLOADER,Malware:FAKEUPDATES,Group:Validation
cc91963aa0fc2841ed47e69e18351cc1	Group:Validation,Malware_Type:DOWNLOADER
ce3aee9c447cecc2907af53a3ab01757	Malware:SUGARLOADER,Group:Validation,Malware_Type:DOWNLOADER
cefd2f5fe51ad9febb3d14cc540a120f	Malware:DUSTMAKER,Group:Validation
cf555a9d6d1b98977aa82ec366860fae	Group:Validation
cf6912e9ff8930c591c9f127caf8db38	Malware:KAITEN,Group:Validation
cfa2265b00222d1b8b1a705c523de49b	Group:Validation,Malware:COILCAGE,Malware_Type:DROPPER_MEMORY_ONLY
d0518aeac1ed98e94631e386ff344c6e	Group:Validation,Malware_Type:DOWNLOADER,Malware:LONGWAIT
d0730e8523f4e88c227ce850a08c0652	Malware:SHUBSTAKE,Malware_Type:DATA_MINER,Group:Validation
d13dae377aad8a602579efb2195e7522	Malware:SHUBSTAKE,Malware_Type:DATA_MINER,Group:Validation
d22d7af49e79dd866a54e08d78c1e5c9	Malware:DUSTMAKER,Group:Validation
d2c4c61684c26bee09782227f81b1c16	Group:Validation,Malware:SLICKDEMON,Malware_Type:DATA_MINER
d2c8d5e70ddc86a6da701902902d36dc	Malware_Type:DATA_MINER,Group:Validation,Malware:SHUBSTAKE
d371888f1bdec26899303772de2803f9	Malware:SLICKDEMON,Group:Validation,Malware_Type:DATA_MINER

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
d395415072d71dd710d3eee9973b229a	Malware:INVISIBLEFERRET,Malware_Type:BACKDOOR,Group:Validation
d3c2bf26bae06f710f9972cdccac4050	Group:Validation
d3dc0e0473cb25c77c34125eb5cc0503	Group:Validation,Malware:SLICKDEMON,Malware_Type:DATA_MINER
d42983c6912acfd3fbe25ca61f3eaa26	Malware:KAITEN,Group:Validation
d4477df4b05a1778579df133d115fd2f	Malware_Type:BACKDOOR,Group:Validation,Malware:SOMBERMEME
d4ed38bf966d4420a1b0a3b1f94c7a46	Malware:BLUEBEAM,Malware:BLUEBEAM.JSP,Group:Validation
d501093d019976600d7110f5cb164446	Malware:DUSTMAKER,Group:Validation
d71708dbb8e9db11ea17b55b9b6c666a	Malware_Type:BACKDOOR,Malware:BADTILE,Group:Validation
da82f261ec4fd828c568c225face8f72	Malware_Type:DOWNLOADER,Group:Validation,Malware:NEONSLIDE
db8b519b3bc88206a3da1d8b3ca261ac	Group:Validation,Malware_Type:DOWNLOADER,Malware:FAKEUPDATES
dbd5937a683052037da3e9267bff9027	Malware:CURLYGATE,Malware_Type:DOWNLOADER,Group:Validation
dd173d2eacd4ba068d0e56ba575d72cb	Malware:REMCOS,Group:Validation,Malware:SHADOWLADDER,Malware_Type:BACKDOOR
dd21d935004e135272e54235c7182e16	Malware_Type:BACKDOOR,Malware:REMCOS,Group:Validation
dd540abaadd01b92bd9ab54ea5bdff1a	Malware:EFSPOTATO,Group:Validation
ddde0463227d2bc573dedfdbcb106a8	Malware_Type:BACKDOOR,Group:Validation
de08f2fe16a54c77a65bfe15c76696e5	Malware:CURLYGATE,Malware_Type:DOWNLOADER,Group:Validation
de9d23d703a25e6059accd3f83b7db09	Malware_Type:BACKDOOR,Malware:REMCOS,Group:Validation
dea57e9dca875b9ea32c892affb237f5	Group:Validation,Malware:BLUEBEAM.JSP
dfbb6b1970144a3278ba4803f0ca601f	Malware:DUSTMAKER,Group:Validation
dffe8577c8d8bbc29eaa62628ab87372	Malware_Type:DOWNLOADER,Malware:FAKEUPDATES,Group:Validation
e0e9d3466bcf81652257164814c7caa0	Group:Validation,Malware:EFSPOTATO

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
e0f2f7a616a9b9885c7c5ee7c09390f3	Malware_Type:BACKDOOR,Malware:REMCOS,Group:Validation
e178725db183476324965e49a9d85268	Group:Validation
e1ca38c706a483a2d1e9187d1468385e	Malware_Type:DOWNLOADER,Group:Validation
e312a0996853c62f61c73dcf3acfab3c	Malware:BADTILE,Malware_Type:BACKDOOR,Group:Validation
e3a54433e38d1592702a3107718099a4	Malware:SANDCLOCK,Group:Validation
e45f1eb4e21a8e10bbff3dc12b92f890	Group:Validation
e490c179d584626c0342ed719217e045	Malware:BADTILE,Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
e53e148d79606788635360ae9ee88ebf	Malware_Type:DOWNLOADER,Group:Validation
e6494c8f60f51f8f0f2730246fccd9cb	Malware_Type:DOWNLOADER,Group:Validation,Malware:CURLYGATE
ea03f8808187d5a27a5c6e96bf673523	Malware:KAITEN,Group:Validation
eab976240725c6368725e48bcd35da50	Group:Validation,Malware:DUSTMAKER
eb66afa3b7f93d3bd93559cf1ee989da	Malware_Type:DOWNLOADER,Malware:FAKEUPDATES,Group:Validation
ebb8cebfb43a0d66668d4483aa96a0b2	Malware:FAKEUPDATES,Group:Validation,Malware_Type:DOWNLOADER
ebcf977806f68af3147e0b78b55f6aed	Malware:MESHAGENT,Group:Validation
efaca8cb92c1460ffcb1d12b933fe01f	Malware_Type:DOWNLOADER,Malware:FAKEUPDATES,Group:Validation
f00d64c64fa66ccfa0679859028ec995	Group:Validation
f025ac2add86fa472da3ddcc540589ec	Group:Validation,Malware:DUSTMAKER
f03a17b69f4c60629ba9b9981c89deb0	Malware:EFSPOTATO,Group:Validation
f0cfe3559bf988d4477a6ac2bcc6c025	Malware_Type:DROPPER,Malware:XWORM,Group:Validation
f160b994ba3ee989be0efb3d6b807fdf	Malware_Type:BACKDOOR,Malware:SHADOWLADDER,Group:Validation,Malware:REMCOS
f164053ab9f96f082865477bdd0463ad	Group:Validation
f18a4e6dda4e84abc18b64e423bf682e	Malware_Type:DOWNLOADER,Malware:FAKEUPDATES,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
f1ec88391dc4b172d15b28b854c3fcea	Malware:EFSPOTATO,Group:Validation
f212e9ad7085cf751acb39ec920b3b11	Group:Validation,Malware:CURLYGATE,Malware_Type:DOWNLOADER
f2500c0cae2e5c3baae4fa5e6b650d93	Malware_Type:DOWNLOADER,Group:Validation,Malware:FAKEUPDATES
f41c391aaf155580a3e2a33d768d8e8e	Malware:HEAVYMETAL,Malware_Type:BACKDOOR,Group:Validation
f45f6f6a90ce5aa47e1ccd7264551c63	Malware:EFSPOTATO,Group:Validation
f54648c6c0d0bd5125f35adc702caa6a	Group:Validation,Malware:DUSTMAKER
f5560871f6002982a6a2cc0b3ee739f7	Malware:SANDCLOCK,Group:Validation
f5e4dbb9b52017446498bc3297da88ac	Malware:MELTRUBY,Malware_Type:BACKDOOR,Group:Validation
f629efff58396f8686ac2c224c76fca5	Malware:HOTAIR,Group:Validation,Malware_Type:INSTALLER
f6a3c8f97b2ef6917787f3995c11b92f	Malware_Type:DOWNLOADER,Malware:FAKEUPDATES,Group:Validation
f7e8c59b200084e1fe299907b4e0f6b5	Malware:PEATWIRE,Group:Validation
f8b1e40ea056845273128f819f778d92	Malware:VIDAR,Malware_Type:DATA_MINER,Group:Validation
f985b8d6d635c266fc4779dad77aa75c	Malware:MELTRUBY,Malware_Type:BACKDOOR,Group:Validation
f997256474fcb9653a19e5220fcc8dc2	Malware:BLUEBEAM.PHP,Group:Validation
fa5884e5ef622428501b100a57e25e5f	Malware:BLUEBEAM.PHP,Group:Validation
fd5844a94443adbd26a65eb22701df22	Malware:COILCAGE,Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
ff53a552d192c4e425fbd6dbde50b212	Malware:REMCOS,Malware_Type:BACKDOOR,Group:Validation,Malware:SHADOWLADDER
ffcc1f9a9a53b706d82b50885d7167c8	Malware:SHUBSTAKE,Malware_Type:DATA_MINER,Group:Validation

Updated Content

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

Supported Operating Systems (OS) and Platforms

VRT used the following environments to test the Validation content included in this update. Each Action is assigned

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

OS/Platform Tags, which you can see when viewing the Action in the Action Library. These tags indicate which environments we expect the Action to run successfully on and are the environments the Actions were tested on.

Mandiant Security Validation Platform

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

Network Actions

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

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.