Mandiant

VHR20260819 - AUGUST 19, 2026

The Mandiant Intelligence Validation Research Team (VRT) has published VHR20260819 - Content Expansion. This content pack requires Director version 4.12.1.0-0 or higher.

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

Summary of Changes

- 68 Actions added
- 59 Files added

Release Highlights

- A new Action covering **Campaign 25-011** (https://advantage.mandiant.com/campaigns/CAMP.25.011), a campaign by **UNC5925** (https://advantage.mandiant.com/actors/UNC5925) that uses fake CAPTCHAs to distribute **NETSUPPORT** (https://advantage.mandiant.com/malware/NETSUPPORT) via **CROSSTRICK** (https://advantage.mandiant.com/malware/CROSSTRICK).
- New Actions demonstrating **Campaign 25-020** (https://advantage.mandiant.com/campaigns/CAMP.25.020), a suspected Russian espionage cluster **UNC6139** (https://advantage.mandiant.com/actors/UNC6139) credential harvesting campaign targeting government and defense entities in Europe using the **BLUEHARVEST** (https://advantage.mandiant.com/malware/BLUEHARVEST) tool.
- New Actions demonstrating **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 and targeting GitHub repositories for unauthorized code modification, utilizing **JADESNOW** (https://advantage.mandiant.com/malware/JADESNOW).
- A new Action demonstrating **Campaign 26-101** (https://advantage.mandiant.com/campaigns/CAMP.26.101), a suspected China-nexus actor **UNC7017** (https://advantage.mandiant.com/actors/UNC7017) campaign involving hijacked software update infrastructure to deliver **SHINYROAD** (https://advantage.mandiant.com/malware/SHINYROAD) and **ADAPTAGENT** (https://advantage.mandiant.com/malware/ADAPTAGENT) payloads to academic and higher education industries.
- New Actions demonstrating **Campaign 26-107** (https://advantage.mandiant.com/campaigns/CAMP.26.107), a suspected Russian espionage campaign by **UNC7005** (https://advantage.mandiant.com/actors/UNC7005) exploiting hospitality Wi-Fi gateways via fake captive portals to redirect web traffic, utilizing tools such as **ANYDESK** (https://advantage.mandiant.com/malware/ANYDESK).
- A new Action covering **Campaign 26-106** (https://advantage.mandiant.com/campaigns/CAMP.26.106), an intrusion campaign by **UNC7003** (https://advantage.mandiant.com/actors/UNC7003) compromising public sector systems using the **SLATEVINE** (https://advantage.mandiant.com/malware/SLATEVINE) backdoor and **IRONBARK** (https://advantage.mandiant.com/malware/IRONBARK) rootkit.
- New Actions covering **Campaign 26-108** (https://advantage.mandiant.com/campaigns/CAMP.26.108), an activity leveraging poisoned NPM dependencies to deploy hidden runtimes and steal GitHub credentials.
- New Actions demonstrating **Campaign 26-109** (https://advantage.mandiant.com/campaigns/CAMP.26.109), an activity by **UNC6267** (https://advantage.mandiant.com/actors/UNC6267) leveraging spearphishing and JavaScript droppers to deploy **NetSupport Manager** (https://advantage.mandiant.com/malware/NETSUPPORT).
- New Actions demonstrating **Campaign 26-114** (https://advantage.mandiant.com/campaigns/CAMP.26.114) by unknown threat actor **UNC6705** (https://advantage.mandiant.com/actors/UNC6705) leveraging ClickFix prompts and PowerShell to deploy **NAILSLY** (https://advantage.mandiant.com/malware/NAILSLY) malware using MSHTA scheduled tasks.
- New Actions demonstrating **Campaign 26-112** (https://advantage.mandiant.com/campaigns/CAMP.26.112), a Suspected China Nexus Actor campaign deploying webshells like **BLUEBEAM.PHP** (https://advantage.mandiant.com/malware/BLUEBEAM.PHP) and privilege escalation tools including **PRINTSPOOFER**

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

(https://advantage.mandiant.com/malware/PRINTSPOOFER).

- New Actions demonstrating **Campaign 24-021** (https://advantage.mandiant.com/campaigns/CAMP.24.021), a financially motivated campaign by **UNC5055** (https://advantage.mandiant.com/actors/UNC5055) distributing **NETSUPPORT** (https://advantage.mandiant.com/malware/NETSUPPORT) payloads using **FAKESMUGGLES** (https://advantage.mandiant.com/malware/FAKESMUGGLES) via drive-by downloads of fake browser updates.
- New Actions demonstrating **Campaign 26-098** (https://advantage.mandiant.com/campaigns/CAMP.26.098), a People's Republic of China-Nexus Espionage Actor **UNC6955** (https://advantage.mandiant.com/actors/UNC6955) campaign utilizing deceptive PDF lures and **HEAVYMETAL** (https://advantage.mandiant.com/malware/HEAVYMETAL) malware to compromise target environments.
- A new Action covering **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.

New Actions

A total of 68 Actions have been added to the content baseline with this update. This includes 68 Network Actions. All Actions in this release are tagged using the MITRE ATT&CK v13 framework.

Network Actions

VID	Name	Tags
A109-238	Command and Control - NAILSLY, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1132,CAMP.26.114,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:NAILSLY,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-239	Command and Control - NAILSLY, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,CAMP.26.114,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:NAILSLY,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-240	Command and Control - UNC5342, JADESNOW, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC5342,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:JADESNOW,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-241	Command and Control - UNC5342, JADESNOW, Communication, Variant #2	ATT&CK:Command and Control,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573,Actor:UNC5342,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:JADESNOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-242	Command and Control - UNC5342, JADESNOW, Registration, Variant #2	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,Actor:UNC5342,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:JADESNOW,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-243	Command and Control - UNC7005, CHERRYPIE, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,Actor:UNC7005,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CHERRYPIE,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-244	Command and Control - UNC7005, CHERRYPIE, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1031,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:M1045,ATT&CK:M1049,ATT&CK:T1027,ATT&CK:T1036.005,ATT&CK:T1071.001,ATT&CK:T1105,Actor:UNC7005,CWE:173,CWE:20,CWE:697,CWE:74,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CHERRYPIE,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-245	Command and Control - UNC7005, CHERRYPIE, 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,ATT&CK:T1105,Actor:UNC7005,CWE:173,CWE:20,CWE:697,CWE:74,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CHERRYPIE,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-246	Malicious File Transfer - BLUEBEAM, BLUEBEAM.PHP, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.112,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.PHP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-247	Malicious File Transfer - BLUEBEAM, BLUEBEAM.PHP, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.112,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEBEAM,Malware:BLUEBEAM.PHP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-248	Malicious File Transfer - IRONBARK, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:IRONBARK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-249	Malicious File Transfer - NAILSLY, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.114,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NAILSLY,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-250	Malicious File Transfer - NAILSLY, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.114,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NAILSLY,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-251	Malicious File Transfer - NAILSLY, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.114,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NAILSLY,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-252	Malicious File Transfer - NETSUPPORT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.24.021,CAMP.25.011,CAMP.25.039,CAMP.26.109,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NETSUPPORT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-253	Malicious File Transfer - NETSUPPORT, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.24.021,CAMP.26.109,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NETSUPPORT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-254	Malicious File Transfer - NETSUPPORT, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.24.021,CAMP.26.109,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NETSUPPORT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-255	Malicious File Transfer - NETSUPPORT, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.109,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NETSUPPORT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-256	Malicious File Transfer - UNC5342, Download, Variant #2	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
A109-257	Malicious File Transfer - UNC5342, Download, Variant #3	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
A109-258	Malicious File Transfer - UNC6139, BLUEHARVEST, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6139,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEHARVEST,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-259	Malicious File Transfer - UNC6139, BLUEHARVEST, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6139,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEHARVEST,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-260	Malicious File Transfer - UNC6139, BLUEHARVEST, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6139,CAMP.25.020,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEHARVEST,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-261	Malicious File Transfer - UNC6139, BLUEHARVEST, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6139,CAMP.25.020,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEHARVEST,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-262	Malicious File Transfer - UNC6139, BLUEHARVEST, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6139,CAMP.25.020,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEHARVEST,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-263	Malicious File Transfer - UNC6139, BLUEHARVEST, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6139,CAMP.25.020,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEHARVEST,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-264	Malicious File Transfer - UNC6139, BLUEHARVEST, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6139,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:BLUEHARVEST,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-265	Malicious File Transfer - UNC6139, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6139,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-266	Malicious File Transfer - UNC6139, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6139,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-267	Malicious File Transfer - UNC6139, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6139,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
A109-268	Malicious File Transfer - UNC6139, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6139,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-269	Malicious File Transfer - UNC6267, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6267,CAMP.26.109,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-270	Malicious File Transfer - UNC6267, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6267,CAMP.26.109,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-271	Malicious File Transfer - UNC6267, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6267,CAMP.26.109,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-272	Malicious File Transfer - UNC6267, NETSUPPORT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6267,CAMP.26.109,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NETSUPPORT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-273	Malicious File Transfer - UNC6267, NETSUPPORT, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6267,CAMP.26.109,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NETSUPPORT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-274	Malicious File Transfer - UNC6267, NETSUPPORT, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6267,CAMP.26.109,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NETSUPPORT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-275	Malicious File Transfer - UNC6267, NETSUPPORT, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6267,CAMP.26.109,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NETSUPPORT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-276	Malicious File Transfer - UNC6557, LOGMEIN, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6557,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:LOGMEIN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-277	Malicious File Transfer - UNC6727, SUNBRICKED, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6727,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SUNBRICKED,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-278	Malicious File Transfer - UNC6727, SUNBRICKED, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6727,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SUNBRICKED,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-279	Malicious File Transfer - UNC6767, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6767,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-280	Malicious File Transfer - UNC6916, DERBSPARK, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6916,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DERBSPARK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-281	Malicious File Transfer - UNC6916, DERBSPARK, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6916,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DERBSPARK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-282	Malicious File Transfer - UNC6916, DERBSPARK, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6916,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DERBSPARK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-283	Malicious File Transfer - UNC6955, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6955,CAMP.26.098,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-284	Malicious File Transfer - UNC6955, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6955,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-285	Malicious File Transfer - UNC6955, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6955,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
A109-286	Malicious File Transfer - UNC6955, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6955,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-287	Malicious File Transfer - UNC6955, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6955,CAMP.26.098,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-288	Malicious File Transfer - UNC6955, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6955,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-289	Malicious File Transfer - UNC6955, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6955,CAMP.26.098,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-290	Malicious File Transfer - UNC6955, HEAVYMETAL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6955,CAMP.26.098,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HEAVYMETAL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-291	Malicious File Transfer - UNC6968, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6968,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-292	Malicious File Transfer - UNC6968, RIBTWIST, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6968,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:RIBTWIST,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-293	Malicious File Transfer - UNC7003, SLATEVINE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7003,CAMP.26.106,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SLATEVINE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-294	Malicious File Transfer - UNC7005, CHERRYPIE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7005,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CHERRYPIE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A109-295	Malicious File Transfer - UNC7005, CHERRYPIE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7005,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CHERRYPIE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-296	Malicious File Transfer - UNC7005, CHERRYPIE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7005,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CHERRYPIE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-297	Malicious File Transfer - UNC7005, CHERRYPIE, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7005,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CHERRYPIE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-298	Malicious File Transfer - UNC7005, CHERRYPIE, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7005,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CHERRYPIE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-299	Malicious File Transfer - UNC7005, CHERRYPIE, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7005,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CHERRYPIE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-300	Malicious File Transfer - UNC7005, PUNCHBOWL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7005,CAMP.26.107,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PUNCHBOWL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-301	Malicious File Transfer - UNC7017, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7017,CAMP.26.101,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-302	Malicious File Transfer - UNC7017, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7017,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-303	Malicious File Transfer - UNC7045, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7045,CAMP.26.108,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
A109-304	Malicious File Transfer - UNC7045, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC7045,CAMP.26.108,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A109-305	Phishing Email - Malicious Attachment, UNC6955, Variant #1	ATT&CK:Initial Access,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:M1049,ATT&CK:M1054,ATT&CK:T1566.001,Actor:UNC6955,Control:Email,NIST:CM-7,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted

New Files

A total of 59 new files have been added to the File Library with this update. This includes 59 malicious files.

Malicious Files

File MD5	Tags
0199319a089670edb47d37e166facb32	Malware:BLUEHARVEST,Group:Validation
03ba1d72088806bcac77d663170aa68d	Group:Validation
0a244ae5e25c45974269f497c927f5b6	Group:Validation
102f33b5a141d6f2f753ffea8abdbc8c	Group:Validation
16b3a38b62dbd622d9ec3d392c4cb7d4	Group:Validation,Malware_Type:WEBSHELL,Malware:SLATEVINE
1768c9971cea4cc10c7dd45a5f8f022a	Malware:NETSUPPORT,Group:Validation
1a4579b5db12cf350055a10497e1be75	Malware:NETSUPPORT,Group:Validation
1b1654131ff974a7cad256f3dd46497f	Group:Validation
2009b69852a9b20bbbe85061e1ef9186	Malware:SUNBRICKED,Malware_Type:DROPPER,Group:Validation
37d72bcdec61009a999cfbe6ae0124ca	Group:Validation
390c964070626a64888d385c514f568e	Group:Validation,Malware:NETSUPPORT
3a86e7d41be609ae0af59f2f526b579b	Malware:CHERRYPIE,Malware_Type:INSTALLER,Group:Validation
4140f7e17e6f97f83aa3472473e01add	Group:Validation
415b1ab4eeb2fe32af2ba80566a395a8	Malware_Type:BACKDOOR,Malware:SUNBRICKED,Group:Validation
464445968e6bf1697d0173708c73c132	Malware:BLUEHARVEST,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
4b40c249f80b73591c7d7623af7275a2	Malware:CHERRYPIE,Malware_Type:INSTALLER,Group:Validation
4d60298bf3ffe62d6c3830f12b2989a1	Malware:CHERRYPIE,Malware_Type:INSTALLER,Group:Validation
4faeeab3d889649be890a422549d4bc6	Group:Validation
53affa1f1995b6a887a21eb9a1829183	Malware:BLUEHARVEST,Group:Validation
5484009071ea96c7b43e8fa052b8d88a	Malware:CHERRYPIE,Malware_Type:INSTALLER,Group:Validation
56727469d879d0114c90143112ee5800	Group:Validation
5b49a3b65f7e3244eb38d552b2580e37	Malware_Type:ROOTKIT,Group:Validation,Malware:IRONBARK
5ce0d80f4e910f2c6c3d6d502bd2ecec	Malware:BLUEBEAM.PHP,Group:Validation
5d721d4eb154602522a86756aea40203	Group:Validation
639eda163fa5a09e93a9793c45d096e8	Malware_Type:LAUNCHER,Malware:RIBTWIST,Group:Validation
726c27a13b6e8b13e92857a8e5902ef8	Group:Validation
72f4fba8005f79c49b6b1a06ceb282d1	Malware_Type:DOWNLOADER,Group:Validation
7698cac577855a5bb5b9ce37bcceb082	Group:Validation,Malware:CROSSROAD
7bcf8d9f6834c44450eac145a967d2f2	Group:Validation
7c5bf2956b76f925136a3c8c893dc38f	Group:Validation,Malware:NETSUPPORT
95a7f2e8ba869fbed79c7ea38457e0b0	Malware:NETSUPPORT,Group:Validation,Malware_Type:UTILITY
9bc2e4c35aa3d281545ccc8b754c3923	Malware_Type:TUNNELER,Malware:DERBSPARK,Group:Validation
9d3f0c3f6d6ca14759683364922926cb	Malware:BLUEHARVEST,Group:Validation
add415fc94270c39957e9abf19e07444	Malware:NAILSLY,Malware_Type:BACKDOOR,Group:Validation
afefbc5f37aad91b8f199bf5fb3b0b68	Malware_Type:TUNNELER,Malware:DERBSPARK,Group:Validation
b2b42fb78c20cea97812740f53ee9f65	Malware_Type:BACKDOOR,Malware:NAILSLY,Group:Validation
b7ca78810c8d30086487771b7347edde	Malware:NETSUPPORT,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
bcc90aaf24c6432b13a33510f617807d	Malware:BLUEBEAM.PHP,Group:Validation
bff79c8c0780ac7bfb64a11fc0b30251	Malware:BLUEHARVEST,Group:Validation
c09684feb319c26c3b66d23728169fe8	Malware_Type:TUNNELER,Malware:DERBSPARK,Group:Validation
c6f4df18cb880500f3921a179c3a3766	Malware:CHERRYPIE,Malware_Type:INSTALLER,Group:Validation
c85e11c90e4eb234e36316a54db3b26b	Malware:LOGMEIN,Group:Validation
c89db988a8b8f84c1d99a8455701f3b5	Group:Validation
cbd49d6649584f73850d558bb782ceda	Malware_Type:BACKDOOR,Malware:NAILSLY,Group:Validation
d557b83f86f0d6e692eb4770a03a306e	Group:Validation
d7a5f86664a007cc1906fc25870e8bbe	Group:Validation
e08c1c97470a3da84af15bb3eb4924dc	Malware:HEAVYMETAL,Group:Validation,Malware_Type:DROPPER
e8d01e8a30ab8c04c0ae9c260fee25bb	Group:Validation
ee75b57b9300aab96530503bfae8a2f2	Group:Validation,Malware:NETSUPPORT
ef024a8e781873570baec2d86827253e	Malware:BLUEHARVEST,Group:Validation
f042dd4e10d3970b68d424b6dd5af473	Group:Validation,Malware:NETSUPPORT
f1686451a1c9a6d819626856c54fd233	Malware:CHERRYPIE,Malware_Type:INSTALLER,Group:Validation
f3388a05b3aeeaac7ca8bd8af1c2f383	Group:Validation
f79c4500de91f11553c5843abd5cfc33	Group:Validation
f84c379cfe6101fcb321e97442a625fe	Group:Validation
f8d026e822cd2896304ca84fcb074c87	Malware:BLUEHARVEST,Group:Validation
fba867df17721879df9d8dcca68d6900	Malware:PUNCHBOWL,Malware_Type:BACKDOOR,Group:Validation
fd270d3a4fde7274d48fce18d76ca337	Group:Validation
fea251a89466c640718aaf74f17501b6	Malware_Type:INSTALLER,Group:Validation

Supported Operating Systems (OS) and Platforms

VRT used the following environments to test the Validation content included in this update. Each Action is assigned OS/Platform Tags, which you can see when viewing the Action in the Action Library. These tags indicate which environments we expect the Action to run successfully on and are the environments the Actions were tested on.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Mandiant

Mandiant Security Validation Platform

System	Build Number / Version
Director	4.11.1.0-95
Actor	4.11.1.0-95

Network Actions

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

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.