Mandiant

VHR20260304 - MARCH 4, 2026

The Mandiant Intelligence Validation Research Team (VRT) has published VHR20260304 - 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

- 72 Actions added
- 30 Files added

Release Highlights

- New Actions demonstrating **Campaign 26-009** (https://advantage.mandiant.com/campaigns/CAMP.26.009), a campaign distributing Node.js-based malware via fake trading installers, utilizing a 'Bring Your Own Interpreter' technique and modifying Windows Defender exclusions.
- New Actions covering **Campaign 26-004** (https://advantage.mandiant.com/campaigns/CAMP.26.004), a financially motivated actor campaign exploiting CrushFTP to deploy TRIDENT ransomware and leveraging **WAVECALL** (https://advantage.mandiant.com/malware/WAVECALL), **SIRENSONG** (https://advantage.mandiant.com/malware/SIRENSONG), and **ANYDESK** (https://advantage.mandiant.com/malware/ANYDESK).
- New Actions demonstrating **Campaign 26-008** (https://advantage.mandiant.com/campaigns/CAMP.26.008), a **TEMP.Hex** (https://advantage.mandiant.com/actors/TEMP.Hex) campaign distributing **SOGU** (https://advantage.mandiant.com/malware/SOGU) via USB flash drives.
- New Actions demonstrating **Campaign 26-007** (https://advantage.mandiant.com/campaigns/CAMP.26.007), a China-nexus threat actor campaign targeting SAP infrastructure for persistence and lateral movement, deploying **POISONPLUG** (https://advantage.mandiant.com/malware/POISONPLUG), **MICROSHELL** (https://advantage.mandiant.com/malware/MICROSHELL), **POISONPLUG.SHADOW** (https://advantage.mandiant.com/malware/POISONPLUG.SHADOW), **SQUASHBUG** (https://advantage.mandiant.com/malware/SQUASHBUG), and **VINEBORER** (https://advantage.mandiant.com/malware/VINEBORER).
- New Actions demonstrating **Campaign 26-012** (https://advantage.mandiant.com/campaigns/CAMP.26.012), a financially motivated campaign leveraging compromised credentials to deploy **AGENDA** (https://advantage.mandiant.com/malware/AGENDA) ransomware and exfiltrate data.
- New Actions demonstrating **Campaign 26-002** (https://advantage.mandiant.com/campaigns/CAMP.26.002), a financially motivated **UNC6590** (https://advantage.mandiant.com/actors/UNC6590) campaign deploying **XMRIG** (https://advantage.mandiant.com/malware/XMRIG) cryptominer and staging **TRUFFLEHOG** (https://advantage.mandiant.com/malware/TRUFFLEHOG) for credential harvesting on Linux servers.
- New Actions demonstrating **Campaign 26-011** (https://advantage.mandiant.com/campaigns/CAMP.26.011), a suspected Iranian espionage group **UNC6446** (https://advantage.mandiant.com/actors/UNC6446) campaign utilizing employment-themed social engineering to distribute **RATTLEPULL** (https://advantage.mandiant.com/malware/RATTLEPULL) and **SUPERSEDAN** (https://advantage.mandiant.com/malware/SUPERSEDAN) malware.
- A new Action covering **Campaign 26-010** (https://advantage.mandiant.com/campaigns/CAMP.26.010), describing how **UNC2565** (https://advantage.mandiant.com/actors/UNC2565) resumed distributing **GOOTLOADER** (https://advantage.mandiant.com/malware/GOOTLOADER) via SEO poisoning and malicious JScript files.
- New Actions covering **DRYNOTE** (https://advantage.mandiant.com/malware/DRYNOTE), a C++ backdoor attributed to **UNC6688** (https://advantage.mandiant.com/actors/UNC6688) that relies on being loaded in memory as raw shellcode.
- New Actions covering **CVE-2025-14847** (https://advantage.mandiant.com/vulnerabilities/CVE-2025-14847), an Improper Handling of Length Parameter Inconsistency vulnerability (MongoBleed) in MongoDB Server allowing sensitive

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

information disclosure.

New Actions

A total of 72 Actions have been added to the content baseline with this update. This includes 29 Network Actions, 13 Host CLI Actions, and 30 Protected Theater Actions. All Actions in this release are tagged using the MITRE ATT&CK v17.1 framework.

Network Actions

VID	Name	Tags
A104-440	Application Vulnerability - CVE-2025-14847, Exploitation, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:M1037,ATT&CK:T1071,CVE-2025-14847,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,NIST:AC-17,NIST:CM-7,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A104-441	Application Vulnerability - CVE-2025-14847, Exploitation, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:M1037,ATT&CK:T1071,CVE-2025-14847,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,NIST:AC-17,NIST:CM-7,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A104-442	Command and Control - TEMP.Hex, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1568,Actor:TEMP.Hex,CAMP.26.008,Control:IDS/IPS,Control:NGFW,Control:Proxy,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-443	Command and Control - TEMP.Hex, SOGU, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,Actor:TEMP.Hex,CAMP.26.008,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SOGU,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-444	Command and Control - UNC6590, XMRIG, Download via Curl, Variant #1	ATT&CK:Command and Control,ATT&CK:Impact,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:M1030,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1489,Actor:UNC6590,CAMP.26.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:XMRIG,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-445	Command and Control - UNC6590, XMRIG, Download via Curl, Variant #2	ATT&CK:Command and Control,ATT&CK:Defense Evasion,ATT&CK:Execution,ATT&CK:M1031,ATT&CK:M1038,ATT&CK:T1014,ATT&CK:T1059.004,ATT&CK:T1071.001,ATT&CK:T1105,Actor:UNC6590,CAMP.26.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:XMRIG,NIST:CM-11,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A104-446	Command and Control - UNC6688, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC6688,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,GLOBAL.26.001,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-447	Command and Control - UNC6688, DRYNOTE, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,Actor:UNC6688,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.001,Malware:DRYNOTE,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-579	Malicious File Transfer - GOOTLOADER, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.010,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:GOOTLOADER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-580	Malicious File Transfer - NESHTA, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.012,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NESHTA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-581	Malicious File Transfer - NETSCAN, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.26.012,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:NETSCAN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-582	Malicious File Transfer - TEMP.Hex, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:TEMP.Hex,CAMP.26.008,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-583	Malicious File Transfer - TEMP.Hex, SOGU, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:TEMP.Hex,CAMP.26.008,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SOGU,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-633	Malicious File Transfer - TEMP.Hex, SOGU, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:TEMP.Hex,CAMP.26.008,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SOGU,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A104-634	Malicious File Transfer - UNC6362, CHILLCHIRP, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6362,CAMP.26.007,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CHILLCHIRP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-635	Malicious File Transfer - UNC6362, POISONPLUG.SHADOW, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6362,CAMP.26.007,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POISONPLUG.SHADOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-638	Malicious File Transfer - UNC6590, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6590,CAMP.26.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-640	Malicious File Transfer - UNC6590, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6590,CAMP.26.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-641	Malicious File Transfer - UNC6590, XMRIG, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6590,CAMP.26.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:XMRIG,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-644	Malicious File Transfer - UNC6688, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6688,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.001,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-645	Malicious File Transfer - UNC6688, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6688,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.001,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-646	Malicious File Transfer - UNC6688, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6688,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.001,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A104-647	Malicious File Transfer - UNC6688, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6688,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.001,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-649	Malicious File Transfer - UNC6688, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6688,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.001,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-650	Malicious File Transfer - UNC6688, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6688,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.001,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-651	Malicious File Transfer - UNC6688, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6688,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.001,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-653	Malicious File Transfer - UNC6688, DRYNOTE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6688,Control:IDS/IPS,Control:NGFW,Control:Proxy,GLOBAL.26.001,Malware:DRYNOTE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A104-654	Phishing Email - Malicious Link, UNC6446, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC6446,CAMP.26.011,Control:Email,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A104-656	Phishing Email - Malicious Link, UNC6446, Variant #2	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC6446,CAMP.26.011,Control:Email,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted

Host CLI Actions

VID	Name	Tags
A104-448	Host CLI - AGENDA, Disable Windows Defender Real Time Monitoring, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.001,CAMP.26.012,CWE:284,Control:Endpoint,Malware:AGENDA,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A104-449	Host CLI - CHRYSALIS, Antivirus Product Discovery via WMI, Variant #1	ATT&CK:Discovery,ATT&CK:T1518.001,Control:Endpoint,GLOBAL.26.001,Malware:CHRYSALIS,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A104-450	Host CLI - CHRYSALIS, System Information Gathering, Variant #1	ATT&CK:Discovery,ATT&CK:T1082,Control:Endpoint,GLOBAL.26.001,Malware:CHRYSALIS,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A104-455	Host CLI - SOGU, TEMP.Hex, Create Hidden Staging Directory, Variant #1	ATT&CK:Defense Evasion,ATT&CK:T1564.001,CAMP.26.008,Control:Endpoint,Malware:SOGU,Malware:TEMP.Hex,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A104-461	Host CLI - UNC2565, GOOTLOADER, Enumerate Volume Shadow Copies, Variant #1	ATT&CK:Discovery,ATT&CK:T1083,Actor:UNC2565,CAMP.26.010,Control:Endpoint,Malware:GOOTLOADER,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,Src:Internal:Trusted
A104-497	Host CLI - UNC2565, RUBEUS, SPN Discovery for Kerberoasting, Variant #1	ATT&CK:Credential Access,ATT&CK:M1026,ATT&CK:M1027,ATT&CK:M1041,ATT&CK:T1558.003,Actor:UNC2565,CAMP.26.010,CWE:200,CWE:326,CWE:327,Control:Endpoint,Malware:RUBEUS,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A104-556	Host CLI - UNC6362, POISONPLUG, Persistence via Masqueraded Service, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC6362,CAMP.26.007,CWE:284,Control:Endpoint,Malware:POISONPLUG,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,Src:Internal:Trusted
A104-557	Host CLI - UNC6446, Obfuscated Local Administrator Group Enumeration, Variant #1	ATT&CK:Discovery,ATT&CK:T1069.001,Actor:UNC6446,CAMP.26.011,Control:Endpoint,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A104-558	Host CLI - UNC6555, Add Account to Local Administrators Group, Variant #1	ATT&CK:M1022,ATT&CK:M1026,ATT&CK:M1028,ATT&CK:M1030,ATT&CK:M1032,ATT&CK:M1042,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1098,Actor:UNC6555,CAMP.26.004,CWE:284,Control:Endpoint,NIST:AC-2,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,Src:Internal:Trusted
A104-559	Host CLI - UNC6555, ANYDESK, Add Firewall Exception, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.004,Actor:UNC6555,CAMP.26.004,Control:Endpoint,Malware:ANYDESK,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,Src:Internal:Trusted
A104-560	Host CLI - UNC6555, Create Backdoor User Account, Variant #1	ATT&CK:M1026,ATT&CK:M1028,ATT&CK:M1030,ATT&CK:M1032,ATT&CK:Persistence,ATT&CK:T1136,Actor:UNC6555,CAMP.26.004,Control:Endpoint,NIST:AC-2,NIST:AC-6,NIST:AU-2,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,Src:Internal:Trusted
A104-561	Host CLI - UNC6679, Adds Windows Defender Exclusion for Current Process, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.001,Actor:UNC6679,CAMP.26.009,CWE:284,Control:Endpoint,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,Src:Internal:Trusted
A104-562	Host CLI - UNC6679, Adds Windows Defender Exclusion for Directory, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.001,Actor:UNC6679,CAMP.26.009,CWE:284,Control:Endpoint,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,Src:Internal:Trusted

Protected Theater Actions

VID	Name	Tags
A104-657	Protected Theater - Add Firewall Rule for Port, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.004,CAMP.26.012,Control:Endpoint,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A104-660	Protected Theater - CHRYSALIS, Persistence via Registry Run Key, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Control:Endpoint,GLOBAL.26.001,Malware:CHRYSALIS,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A104-661	Protected Theater - Defense Evasion by Renaming Tools, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:T1036.003,CAMP.26.002,Control:Endpoint,OS:Linux:Ubuntu,RunAs:Root,Src:Internal:Trusted
A104-962	Protected Theater - GOOTLOADER, Enumerate Volume Shadow Copies, Variant #1	ATT&CK:Discovery,ATT&CK:T1082,CAMP.26.010,Control:Endpoint,Malware:GOOTLOADER,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A105-256	Protected Theater - Persistence via Systemd Service, Variant #3	ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1026,ATT&CK:M1033,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.002,CAMP.26.002,Control:Endpoint,OS:Linux:Ubuntu,RunAs:Root,Src:Internal:Trusted
A105-257	Protected Theater - Rename System Binaries for Defense Evasion, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:T1036.003,CAMP.26.002,Control:Endpoint,OS:Linux:Ubuntu,RunAs:Root,Src:Internal:Trusted
A105-775	Protected Theater - TEMP.Hex, SOGU.JSPS, Create and Run Scheduled Task, Variant #1	ATT&CK:Execution,ATT&CK:M1018,ATT&CK:M1026,ATT&CK:M1028,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1053.005,Actor:TEMP.Hex,CAMP.26.008,Control:Endpoint,Malware:SOGU.JSPS,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A106-317	Protected Theater - TEMP.Hex, SOGU.JSPS, Delete Scheduled Tasks, Variant #1	ATT&CK:Defense Evasion,ATT&CK:T1070.004,Actor:TEMP.Hex,CAMP.26.008,Control:Endpoint,Malware:SOGU.JSPS,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A106-433	Protected Theater - TEMP.Hex, SOGU.JSPS, Drop Nerowaveedit.dat, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1013,ATT&CK:M1051,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1073,ATT&CK:T1574.002,Actor:TEMP.Hex,CAMP.26.008,CWE:114,CWE:706,Control:Endpoint,Malware:SOGU.JSPS,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A106-655	Protected Theater - TEMP.Hex, SOGU.JSPS, Executes to copy itself, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1013,ATT&CK:M1051,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1574.002,Actor:TEMP.Hex,CAMP.26.008,CWE:114,CWE:706,Control:Endpoint,Malware:SOGU.JSPS,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A106-656	Protected Theater - TEMP.Hex, SOGU.JSPS, Execution, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1038,ATT&CK:M1044,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1574.001,Actor:TEMP.Hex,CAMP.26.008,CWE:114,CWE:427,Control:Endpoint,Malware:SOGU.JSPS,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A106-657	Protected Theater - TEMP.Hex, SOGU.WD, Drops AvastAuth.dat, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1038,ATT&CK:M1044,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1574.001,Actor:TEMP.Hex,CAMP.26.008,CWE:114,CWE:427,Control:Endpoint,Malware:SOGU.WD,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A106-796	Protected Theater - TEMP.Hex, SOGU.WD, Drops wsc.dll, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1013,ATT&CK:M1051,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1574.002,Actor:TEMP.Hex,CAMP.26.008,CWE:114,CWE:706,Control:Endpoint,Malware:SOGU.WD,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A106-802	Protected Theater - TEMP.Hex, SOGU.WD, Execution and Drop of wsc.dll to ProgramData, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1013,ATT&CK:M1051,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1574.002,Actor:TEMP.Hex,CAMP.26.008,CWE:114,CWE:706,Control:Endpoint,Malware:SOGU.WD,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A106-924	Protected Theater - TEMP.Hex, SOGU.WD, Execution, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1038,ATT&CK:M1044,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1574.001,Actor:TEMP.Hex,CAMP.26.008,CWE:114,CWE:427,Control:Endpoint,Malware:SOGU.WD,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-395	Protected Theater - TEMP.Hex, SOGU.WD, Execution, Variant #2	ATT&CK:Defense Evasion,ATT&CK:M1038,ATT&CK:M1044,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1574.001,Actor:TEMP.Hex,CAMP.26.008,CWE:114,CWE:427,Control:Endpoint,Malware:SOGU.WD,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-408	Protected Theater - UNC6590, XMRIG, Service Activation (Enable Only), Variant #1	ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1026,ATT&CK:M1033,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.002,Actor:UNC6590,CAMP.26.002,Control:Endpoint,Malware:XMRIG,OS:Linux:Ubuntu,RunAs:Root,Src:Internal:Trusted
A107-492	Protected Theater - UNC6590, XMRIG, Service Activation (Enable Only), Variant #2	ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1026,ATT&CK:M1033,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.002,Actor:UNC6590,CAMP.26.002,Control:Endpoint,Malware:XMRIG,OS:Linux:Ubuntu,RunAs:Root,Src:Internal:Trusted
A107-493	Protected Theater - UNC6688, DRYNOTE, Drops Backdoor, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6688,Control:Endpoint,GLOBAL.26.001,Malware:DRYNOTE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-494	Protected Theater - UNC6688, DRYNOTE, Execution, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1038,ATT&CK:M1044,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1574.001,Actor:UNC6688,CWE:114,CWE:427,Control:Endpoint,GLOBAL.26.001,Malware:DRYNOTE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-495	Protected Theater - UNC6688, DRYNOTE, Execution, Variant #2	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6688,Control:Endpoint,GLOBAL.26.001,Malware:DRYNOTE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-496	Protected Theater - UNC6688, DRYNOTE, Execution, Variant #3	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC6688,CWE:284,Control:Endpoint,GLOBAL.26.001,Malware:DRYNOTE,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A107-497	Protected Theater - UNC6688, DRYNOTE, Install BluetoothService, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC6688,CWE:284,Control:Endpoint,GLOBAL.26.001,Malware:DRYNOTE,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-498	Protected Theater - UNC6688, DRYNOTE, Uninstalls Persistence Service, Variant #1	ATT&CK:Defense Evasion,ATT&CK:T1070.004,Actor:UNC6688,Control:Endpoint,GLOBAL.26.001,Malware:DRYNOTE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-499	Protected Theater - UNC6688, Google Update Service, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC6688,CWE:284,Control:Endpoint,GLOBAL.26.001,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-500	Protected Theater - UNC6688, Installer Execution, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6688,Control:Endpoint,GLOBAL.26.001,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-501	Protected Theater - UNC6688, Malware Execution, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6688,Control:Endpoint,GLOBAL.26.001,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-502	Protected Theater - UNC6688, Malware Execution, Variant #2	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6688,Control:Endpoint,GLOBAL.26.001,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-503	Protected Theater - UNC6688, Malware Execution, Variant #3	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6688,Control:Endpoint,GLOBAL.26.001,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A107-504	Protected Theater - UNC6688, Stage Files for DLL Sideloading, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1013,ATT&CK:M1051,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1574.002,Actor:UNC6688,CWE:114,CWE:706,Control:Endpoint,GLOBAL.26.001,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

New Files

A total of 30 new files have been added to the File Library with this update. This includes 30 malicious files.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Malicious Files

File MD5	Tags
10a22fc98ce4b716a8347fb23ab0fb2d	Group:Validation
170e8c92111a6234c3d663e9a35f7f86	Group:Validation
28cb7b261f4eb97e8a4b3b0d32f8def1	Group:Validation
32f3c40b0ed1c5cf23430be7f9eb7b06	Malware_Type:LAUNCHER,Group:Validation
51b507bc038831b32e6d457028ec0368	Malware:NESHTA,Group:Validation
53830fe278811363f93e0906d8b5ce69	Group:Validation,Malware_Type:BACKDOOR,Malware:SOGU
55921689bddd723f95f1a1e9b8f782e2	Malware_Type:BACKDOOR,Group:Validation,Malware:DRYNOTE
5fd1bc7952d23f89ae10e37ce562c38e	Malware_Type:LAUNCHER,Malware:XMRIG,Group:Validation
6aed7e49bd6c10c4eaee34f8c0eaa055	Group:Validation
755a273159c2b1e9031fa0dfbd0514a4	Group:Validation
774146bd58327c25fb5c86f9eca3b07d	Malware:XMRIG,Group:Validation
831252e7fa9bd6fa174715647ebce516	Group:Validation,Malware:SOGU,Malware_Type:LAUNCHER
8523131ead4e01b864a2d7100b77fe0d	Group:Validation
869b85d8004b64fbef4d4ae9d4b20f00	Group:Validation
87f1184c3ba77b8dfe156113d432d7ad	Malware:NETSCAN,Group:Validation
8dd8afbd1e8bbea5723b5f24e541bc58	Malware_Type:BACKDOOR,Malware:CHILLCHIRP,Group:Validation
916210d9192601e463096104f0889fe3	Malware:GOOTLOADER,Malware_Type:DOWNLOADER,Group:Validation
9d663237dc9c2ab875c7554675311c93	Group:Validation
a27c71688c34561491c648f99f5e2e22	Malware_Type:BACKDOOR,Malware:POISONPLUG.SHADOW,Group:Validation
aa304ec2149205ee9edef737bf1ad0a2	Group:Validation
ab6daaf5fee71ebd88d5ba3ae2168723	Group:Validation
b524722db5a0f45718394b1217f02138	Group:Validation
b528771daa269af307e87f73016d6d49	Group:Validation,Malware_Type:INSTALLER
bca4096d5fa7cf08d1f902a894d2d2be	Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
c1b1cad9e7afabfacd8988c2a6182a20	Group:Validation
cd56b29fba7e3bc6fb0ae684637f52cc	Group:Validation,Malware:SOGU.JSPS,Malware_Type:BACKDOOR
cf51dbe3926ba5e288fee3f17ef73aa7	Group:Validation
d6fa5813e23ebbb30cd0eba5dba98766	Group:Validation
d7ce7125e38d4d79cb65541edbccb4a0	Malware_Type:LAUNCHER,Malware:XMRIG,Group:Validation
e776de5a5ab104ba814d6a70c27ecc42	Group:Validation

Supported Operating Systems (OS) and Platforms

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

Mandiant Security Validation Platform

System	Build Number / Version
Director	4.14.4.1-51
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.