Mandiant

# VHR20260204 - FEBRUARY 4, 2026

The Mandiant Intelligence Validation Research Team (VRT) has published VHR20260204 - 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

- 50 Actions added
- 30 Files added

## Release Highlights

- 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 organizations in Azerbaijan and Turkey.
- New Actions detailing **Campaign 25-080** (https://advantage.mandiant.com/campaigns/CAMP.25.080), a campaign by **UNC6560** (https://advantage.mandiant.com/actors/UNC6560) that leverages **CVE-2025-59287** (https://advantage.mandiant.com/vulnerabilities/CVE-2025-59287) for payload delivery and persistence of **POISONPLUG.SHADOW** (https://advantage.mandiant.com/malware/POISONPLUG.SHADOW).
- New Actions covering **Campaign 25-081** (https://advantage.mandiant.com/campaigns/CAMP.25.081), a campaign by **UNC6553** (https://advantage.mandiant.com/actors/UNC6553) leveraging **SURFCAKE** (https://advantage.mandiant.com/malware/SURFCAKE) to gain initial access and deliver additional malware.
- New Actions demonstrating **Campaign 25-085** (https://advantage.mandiant.com/campaigns/CAMP.25.085), a campaign by financially motivated actors exploiting **CVE-2025-55182** (https://advantage.mandiant.com/vulnerabilities/CVE-2025-55182) to deploy **XMRIG** (https://advantage.mandiant.com/malware/XMRIG) cryptominers.
- A new Action demonstrating **Campaign 25-072** (https://advantage.mandiant.com/campaigns/CAMP.25.072), a financially motivated actor **UNC6357** (https://advantage.mandiant.com/actors/UNC6357) campaign leveraging Microsoft SharePoint vulnerabilities and deploying **LOCKBIT** (https://advantage.mandiant.com/malware/LOCKBIT) ransomware.
- New Actions demonstrating **Campaign 26-001** (https://advantage.mandiant.com/campaigns/CAMP.26.001), a campaign by financially motivated actor **UNC6602** (https://advantage.mandiant.com/actors/UNC6602) exploiting **CVE-2025-55182** (https://advantage.mandiant.com/vulnerabilities/CVE-2025-55182) and deploying **HOTTEA** (https://advantage.mandiant.com/malware/HOTTEA) malware to hijack Nginx for malicious redirects.
- New Actions demonstrating **Campaign 25-088** (https://advantage.mandiant.com/campaigns/CAMP.25.088), an unknown threat actor **UNC6599** (https://advantage.mandiant.com/actors/UNC6599) campaign targeting MacOS systems via **ATOMICPROMPT** (https://advantage.mandiant.com/malware/ATOMICPROMPT).

## New Actions

A total of 50 Actions have been added to the content baseline with this update. This includes 36 Network Actions, 7 Host CLI Actions, and 7 Protected Theater Actions. All Actions in this release are tagged using the MITRE ATT&CK v17 framework.

### Network Actions

| VID | Name | Tags |
|---|---|---|

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

| VID | Name | Tags |
|---|---|---|
| A104-058 | Command and Control - UNC1549, TWOSTROKE, C2 Traffic, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC1549,CAMP.25.082,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-061 | Command and Control - UNC1549, TWOSTROKE, C2 Traffic, Variant #2 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1001,ATT&CK:T1071.001,Actor:UNC1549,CAMP.25.082,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,Malware:TWOSTROKE,NIST:AC-4,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-063 | Command and Control - UNC1549, TWOSTROKE, C2 Traffic, Variant #3 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC1549,CAMP.25.082,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-064 | Command and Control - UNC1549, TWOSTROKE, 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:UNC1549,CAMP.25.082,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-065 | Command and Control - UNC6602, HOTTEA, C2, 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,ATT&CK:T1105,Actor:UNC6602,CAMP.26.001,CWE:173,CWE:20,CWE:697,CWE:74,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTTEA,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-075 | Malicious File Transfer - DCSYNCER, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.25.072,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:DCSYNCER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-076 | Malicious File Transfer - FRP, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.25.072,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:FRP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-077 | Malicious File Transfer - IMPACKET, PSEXEC, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.25.072,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:IMPACKET,Malware:PSEXEC,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

| VID | Name | Tags |
|---|---|---|
| A104-078 | Malicious File Transfer - MASSCAN, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.25.072,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MASSCAN,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-079 | Malicious File Transfer - MIMIKATZ, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.25.072,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MIMIKATZ,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-080 | Malicious File Transfer - PETITPOTAM, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.25.072,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:PETITPOTAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-086 | Malicious File Transfer - SHARPHOSTINFO, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.25.072,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SHARPHOSTINFO,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-087 | Malicious File Transfer - SUO5, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,CAMP.25.072,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SUO5,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-110 | Malicious File Transfer - UNC1549, CREDSTROKE, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CREDSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-111 | Malicious File Transfer - UNC1549, CREDSTROKE, Download, Variant #2 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:CREDSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-112 | Malicious File Transfer - UNC1549, MAILMUSTER, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MAILMUSTER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

| VID | Name | Tags |
|---|---|---|
| A104-115 | Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-117 | Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #2 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-142 | Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #3 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-151 | Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #4 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,CAMP.25.082,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-170 | Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #5 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-172 | Malicious File Transfer - UNC1549, TWOSTROKE, Download, Variant #6 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1549,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:TWOSTROKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-182 | Malicious File Transfer - UNC6357, HAMMERDROP, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6357,CAMP.25.072,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HAMMERDROP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-183 | Malicious File Transfer - UNC6553, SURFCAKE, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6553,CAMP.25.081,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SURFCAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

| VID | Name | Tags |
|---|---|---|
| A104-202 | Malicious File Transfer - UNC6560, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6560,CAMP.25.080,Control:IDS/IPS,Control:NGFW,Control:Proxy,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-209 | Malicious File Transfer - UNC6560, POISONPLUG.SHADOW, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6560,CAMP.25.080,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:POISONPLUG.SHADOW,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-247 | Malicious File Transfer - UNC6586, SNOWLIGHT, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6586,CAMP.25.084,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SNOWLIGHT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-346 | Malicious File Transfer - UNC6586, SNOWLIGHT, Download, Variant #2 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6586,CAMP.25.084,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:SNOWLIGHT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-347 | Malicious File Transfer - UNC6595, ANGRYREBEL.LINUX, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6595,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ANGRYREBEL.LINUX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-348 | Malicious File Transfer - UNC6599, ATOMIC, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6599,CAMP.25.088,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATOMIC,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-349 | Malicious File Transfer - UNC6599, ATOMICPROMPT, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6599,CAMP.25.088,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:ATOMICPROMPT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-350 | Malicious File Transfer - UNC6600, MINOCAT, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6600,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:MINOCAT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

| VID | Name | Tags |
| --- | --- | --- |
| A104-351 | Malicious File Transfer - UNC6602, HOTTEA, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6602,CAMP.26.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTTEA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-358 | Malicious File Transfer - UNC6602, HOTTEA, Download, Variant #2 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6602,CAMP.26.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTTEA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-368 | Malicious File Transfer - UNC6602, HOTTEA, Download, Variant #3 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6602,CAMP.26.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HOTTEA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |
| A104-369 | Malicious File Transfer - UNC6603, HISONIC, Download, Variant #1 | ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6603,Control:IDS/IPS,Control:NGFW,Control:Proxy,Malware:HISONIC,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted |

Host CLI Actions

| VID | Name | Tags |
| --- | --- | --- |
| A104-066 | Host CLI - UNC1549, TWOSTROKE, Create 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:UNC1549,CAMP.25.082,Control:Endpoint,Malware:TWOSTROKE,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted |
| A104-067 | Host CLI - UNC6357, Create Service for WinPcap Persistence, Variant #1 | ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC6357,CAMP.25.072,CWE:284,Control:Endpoint,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted |
| A104-068 | Host CLI - UNC6553, SURFCAKE, Persistence via Registry Run Key, Variant #1 | ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC6553,CAMP.25.081,Control:Endpoint,Malware:SURFCAKE,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 |
| --- | --- | --- |
| A104-069 | Host CLI - UNC6585, XMRIG, Create Systemd Service for Persistence, 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:UNC6585,CAMP.25.085,Control:Endpoint,Malware:XMRIG,OS:Linux:CentOS,OS:Linux:Ubuntu,RunAs:Root,Src:Internal:Trusted |
| A104-070 | Host CLI - UNC6586, SNOWLIGHT, Execute with Nohup, Variant #1 | ATT&CK:Defense Evasion,ATT&CK:T1564.011,Actor:UNC6586,CAMP.25.084,Control:Endpoint,Malware:SNOWLIGHT,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted |
| A104-073 | Host CLI - UNC6586, SNOWLIGHT, Make Payload Executable, Variant #1 | ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1026,ATT&CK:T1222.002,Actor:UNC6586,CAMP.25.084,Control:Endpoint,Malware:SNOWLIGHT,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted |
| A104-074 | Host CLI - UNC6586, SNOWLIGHT, Obfuscated Command, Variant #1 | ATT&CK:Defense Evasion,ATT&CK:T1027.010,Actor:UNC6586,CAMP.25.084,Control:Endpoint,Malware:SNOWLIGHT,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted |

Protected Theater Actions

| VID | Name | Tags |
| --- | --- | --- |
| A104-370 | Protected Theater - SNOWLIGHT, Make Payload Executable, Variant #1 | ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1026,ATT&CK:T1222.002,CAMP.25.084,Control:Endpoint,Malware:SNOWLIGHT,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted |
| A104-371 | Protected Theater - SNOWLIGHT, Nohup Execution, Variant #1 | ATT&CK:Defense Evasion,ATT&CK:T1564.011,CAMP.25.084,Control:Endpoint,Malware:SNOWLIGHT,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted |
| A104-372 | Protected Theater - UNC1549, TWOSTROKE, Execution, Variant #1 | ATT&CK:Defense Evasion,ATT&CK:Execution,ATT&CK:M1013,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:M1051,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1204.002,ATT&CK:T1574.002,Actor:UNC1549,CAMP.25.082,CWE:114,CWE:706,Control:Endpoint,Malware:TWOSTROKE,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 |
|---|---|---|
| A104-392 | Protected Theater - UNC1549, TWOSTROKE, Execution, Variant #2 | ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC1549,CAMP.25.082,Control:Endpoint,Malware:TWOSTROKE,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 |
| A104-430 | Protected Theater - UNC1549, TWOSTROKE, 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:UNC1549,CAMP.25.082,Control:Endpoint,Malware:TWOSTROKE,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 |
| A104-436 | Protected Theater - UNC6585, XMRIG, Persistence, 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:UNC6585,CAMP.25.085,Control:Endpoint,Malware:XMRIG,OS:Linux:Ubuntu,RunAs:Root,Src:Internal:Trusted |
| A104-438 | Protected Theater - UNC6602, Web Server Configuration Modification, Variant #1 | ATT&CK:Command and Control,ATT&CK:Initial Access,ATT&CK:T1659,Actor:UNC6602,CAMP.26.001,Control:Endpoint,OS:Linux:Ubuntu,RunAs:Root,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.

### Malicious Files

| File MD5 | Tags |
|---|---|
| 0522ba68fa6159abc7d00172e732088d | Malware:HOTTEA,Group:Validation |
| 097447c4b526f8a42e3144afe510ec20 | Malware_Type:BACKDOOR,Group:Validation,Malware:TWOSTROKE |
| 0d88403781dc02fdac7866e83b8a0439 | Malware_Type:BACKDOOR,Group:Validation,Malware:TWOSTROKE |
| 10231e4c2ade4f21c9d4fa52cabc8b5e | Malware_Type:BACKDOOR,Group:Validation,Malware:HISONIC |
| 27e00b5594530e8c5e004098eef2ec50 | Malware_Type:LAUNCHER,Malware:POISONPLUG.SHADOW,Group:Validation |
| 37197e5ed67443b01c8bc7f1249cba6a | Malware:CREDSTROKE,Group:Validation |
| 405e251f8fa333f48872cd04577731ec | Group:Validation |
| 453b923b556ae6fd03a59e37e3797011 | Group:Validation,Malware:PETITPOTAM,Tool_Type:DRIVER |

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

| File MD5 | Tags |
| --- | --- |
| 50300de5e4786530ea603224ccbcbb02 | Malware:MIMIKATZ,Group:Validation |
| 533585eb6a8a4aad2ad09bbf272eb45b | Malware_Type:TUNNELER,Malware:MINOCAT,Group:Validation |
| 68abbdd75f82a22e3cf6200e13a664b3 | Malware_Type:DATA_MINER,Malware:MAILMUSTER,Group:Validation |
| 6c079cd29e7c594dcf536b782cc9cea0 | Malware_Type:LAUNCHER,Malware:HOTTEA,Group:Validation |
| 6d9b590d3666597c338c518e21fbf4ee | Malware:HAMMERDROP,Malware_Type:DROPPER,Group:Validation |
| 6edce6c34434fbf2a3491e60534fda0a | Malware:SHARPHOSTINFO,Malware_Type:UTILITY,Group:Validation |
| 80c91b4343fe1260e348872e1b4c0713 | Malware_Type:BACKDOOR,Group:Validation,Malware:TWOSTROKE |
| 83100a20cae2649fd8d0400c96b267fe | Malware:CREDSTROKE,Group:Validation |
| a4093613f597671cc23a6dec5567b815 | Malware_Type:TUNNELER,Malware:SUO5,Group:Validation |
| be556a0d7d75524acc5518482e43ed9a | Malware_Type:BACKDOOR,Group:Validation,Malware:TWOSTROKE |
| c563056e9b3bea79262c49fe3974b92f | Malware:PSEXEC,Malware:IMPACKET,Group:Validation |
| caff3c75546a9f69d5b7e2002ce01963 | Malware:DCSYNCER,Group:Validation |
| cbf4f812b6790c98bd1dc7eaf45ca696 | Group:Validation |
| cce413881e131798a11bc89a8d4707b1 | Malware:ATOMIC,Group:Validation |
| cea48192aab6af327c6596c069c0f778 | Malware_Type:DOWNLOADER,Malware:ATOMICPROMPT,Group:Validation |
| cef266a5ea7ba57abc576cbeb5497c97 | Malware_Type:BACKDOOR,Malware:TWOSTROKE,Group:Validation |
| d0f9e9a9d35b6573f713cb2ffacacfdb | Malware:SURFCAKE,Group:Validation,Malware_Type:DOWNLOADER |
| e1a40afd9a07710f0aa7085271433350 | Malware_Type:DOWNLOADER,Malware:SNOWLIGHT,Group:Validation |
| e370c0a29ff9c917b63627e3f7b719d7 | Malware:ANGRYREBEL.LINUX,Malware_Type:BACKDOOR,Group:Validation |
| e543a7945090d0806d270780ea288011 | Malware:FRP,Group:Validation |
| e5f0aea43ac33bf19a78c1a600f690d5 | Malware_Type:BACKDOOR,Malware:TWOSTROKE,Group:Validation |

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

| File MD5 | Tags |
| --- | --- |
| ea41660477ce24b12626b861f616c46d | Malware:MASSCAN,Group:Validation |

## Supported Operating Systems (OS) and Platforms

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

### Mandiant Security Validation Platform

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

### Network Actions

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

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.