Mandiant

VHR20260407 | M-TRENDS 2026 - APRIL 7, 2026

The Mandiant Intelligence Validation Research Team (VRT) has published VHR20260407 - 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

- 300 Actions added
- 191 Files added
- 274 Actions updated

Release Highlights

- New Actions related to the Actors, Malware, and Vulnerabilities in the **M-Trends 2026 Report** (https://cloud.google.com/security/resources/m-trends?hl=en). The M-Trends 2026 Report provides trends analysis, metrics, and learnings drawn from the frontlines of Mandiant incident response investigations and threat intelligence findings between January 1, 2025 - December 31, 2025.

New Actions

A total of 300 Actions have been added to the content baseline with this update. This includes 212 Network Actions, 35 Host CLI Actions, and 53 Protected Theater Actions. All Actions in this release are tagged using the MITRE ATT&CK v17.1 framework. The content pack also expands our coverage of the MITRE ATT&CK Framework and includes 5 new Techniques.

Network Actions

VID	Name	Tags
A108-084	Malicious File Transfer - ADAPTAGENT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:ADAPTAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-085	Malicious File Transfer - ADAPTAGENT, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:ADAPTAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-086	Command and Control - ADAPTAGENT, Tasking, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:ADAPTAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-087	Command and Control - ADAPTAGENT, Tasking, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:ADAPTAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-088	Command and Control - ADAPTAGENT, Tasking, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:ADAPTAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-089	Command and Control - ADAPTAGENT, Tasking, Variant #5	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,M-Trends 2026,Malware:ADAPTAGENT,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-090	Malicious File Transfer - ADAPTAGENT, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:ADAPTAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-091	Command and Control - ADAPTAGENT, Exfiltration, Variant #2	ATT&CK:Command and Control,ATT&CK:M1030,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,ATT&CK:T1571,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:ADAPTAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-092	Command and Control - ADAPTAGENT, Exfiltration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:ADAPTAGENT,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-093	Command and Control - ADAPTAGENT, Tasking, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,M-Trends 2026,Malware:ADAPTAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-094	Malicious File Transfer - REDBIKE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:REDBIKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-095	Malicious File Transfer - UNC6021, REDBIKE, REDBIKE.LINUX, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6021,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:REDBIKE,Malware:REDBIKE.LINUX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-096	Command and Control - ADAPTAGENT, Tasking, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:ADAPTAGENT,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-097	Malicious File Transfer - JSPKIT, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:JSPKIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-098	Malicious File Transfer - JSPKIT, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:JSPKIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-099	Command and Control - ADAPTAGENT, Tasking, Variant #9	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,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:ADAPTAGENT,NIST:CM-11,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-100	Malicious File Transfer - UNC6303, ADAPTAGENT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6303,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:ADAPTAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-101	Command and Control - ADAPTAGENT, Tasking, Variant #10	ATT&CK:Command and Control,ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1031,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1071.001,ATT&CK:T1105,ATT&CK:T1204.002,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:ADAPTAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-102	Command and Control - ADAPTAGENT, Tasking, Variant #3	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,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:ADAPTAGENT,NIST:CM-11,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-103	Command and Control - ADAPTAGENT, Tasking, Variant #12	ATT&CK:Command and Control,ATT&CK:Execution,ATT&CK:Initial Access,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:M1048,ATT&CK:M1050,ATT&CK:M1051,ATT&CK:T1071.001,ATT&CK:T1189,ATT&CK:T1203,CWE:119,CWE:79,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:ADAPTAGENT,NIST:CM-5,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-104	Command and Control - ADAPTAGENT, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:ADAPTAGENT,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-105	Command and Control - ADAPTAGENT, Tasking, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:ADAPTAGENT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-106	Malicious File Transfer - REDBIKE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:REDBIKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-107	Malicious File Transfer - JSPKIT, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:JSPKIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-109	Malicious File Transfer - JSPKIT, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:JSPKIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-110	Malicious File Transfer - JSPKIT, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:JSPKIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-111	Malicious File Transfer - JSPKIT, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:JSPKIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-112	Malicious File Transfer - JSPKIT, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:JSPKIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-114	Command and Control - SYSTEMBC, SYSTEMBC.V2, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:M1037,ATT&CK:T1071.001,ATT&CK:T1090.003,CWE:287,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SYSTEMBC,Malware:SYSTEMBC.V2,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-115	Malicious File Transfer - JSPKIT, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:JSPKIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-116	Malicious File Transfer - AMADEY, SYSTEMBC, SYSTEMBC.V2, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:AMADEY,Malware:SYSTEMBC,Malware:SYSTEMBC.V2,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-117	Command and Control - AMADEY, LUMMAC.V2, SYSTEMBC, SYSTEMBC.V2, 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,M-Trends 2026,Malware:AMADEY,Malware:LUMMAC.V2,Malware:SYSTEMBC,Malware:SYSTEMBC.V2,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-118	Malicious File Transfer - JSPKIT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:JSPKIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-119	Malicious File Transfer - AMADEY, LUMMAC, LUMMAC.V2, SYSTEMBC, SYSTEMBC.V2, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:AMADEY,Malware:LUMMAC,Malware:LUMMAC.V2,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
A108-121	Command and Control - AMADEY, SYSTEMBC, SYSTEMBC.V2, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,M-Trends 2026,Malware:AMADEY,Malware:SYSTEMBC,Malware:SYSTEMBC.V2,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-122	Malicious File Transfer - SYSTEMBC, SYSTEMBC.V2, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SYSTEMBC,Malware:SYSTEMBC.V2,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-123	Command and Control - BEACON.STAGER, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1030,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1571,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:BEACON.STAGER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-124	Command and Control - AMADEY, LUMMAC.V2, SYSTEMBC, SYSTEMBC.V2, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,M-Trends 2026,Malware:AMADEY,Malware:LUMMAC.V2,Malware:SYSTEMBC,Malware:SYSTEMBC.V2,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-125	Command and Control - AMADEY, LUMMAC.V2, SYSTEMBC, SYSTEMBC.V2, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1020,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1573,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,M-Trends 2026,Malware:AMADEY,Malware:LUMMAC.V2,Malware:SYSTEMBC,Malware:SYSTEMBC.V2,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-126	Malicious File Transfer - SYSTEMBC, SYSTEMBC.PERL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SYSTEMBC,Malware:SYSTEMBC.PERL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-127	Malicious File Transfer - AGENDA, NESHTA, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:AGENDA,Malware:NESHTA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-129	Malicious File Transfer - BRICKSTORM, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:BRICKSTORM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-130	Malicious File Transfer - KRABDRIP, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:KRABDRIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-131	Malicious File Transfer - UNC5932, KRABDRIP, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5932,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:KRABDRIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-132	Malicious File Transfer - UNC5221, SPAWNSNARE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5221,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SPAWNSNARE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-133	Malicious File Transfer - KRABDRIP, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:KRABDRIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-134	Malicious File Transfer - KRABDRIP, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:KRABDRIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-135	Malicious File Transfer - KRABDRIP, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:KRABDRIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-136	Malicious File Transfer - UNC5932, KRABDRIP, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5932,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:KRABDRIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-137	Malicious File Transfer - UNC6301, KRABDRIP, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6301,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:KRABDRIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-138	Malicious File Transfer - KRABDRIP, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:KRABDRIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-139	Malicious File Transfer - KRABDRIP, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:KRABDRIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-140	Malicious File Transfer - KRABDRIP, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:KRABDRIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-141	Malicious File Transfer - KRABDRIP, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:KRABDRIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-142	Malicious File Transfer - KRABDRIP, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:KRABDRIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-143	Malicious File Transfer - KRABDRIP, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:KRABDRIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-144	Malicious File Transfer - AGENDA, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:AGENDA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-145	Malicious File Transfer - AGENDA, Download, Variant #13	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:AGENDA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-146	Command and Control - KRABDRIP, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:Discovery,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1082,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:KRABDRIP,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-147	Malicious File Transfer - UNC5932, KRABDRIP, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5932,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:KRABDRIP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-148	Malicious File Transfer - AGENDA, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:AGENDA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-149	Malicious File Transfer - AGENDA, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:AGENDA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-150	Malicious File Transfer - INC, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:INC,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-151	Malicious File Transfer - INC, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:INC,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-152	Malicious File Transfer - INC, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:INC,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-154	Malicious File Transfer - INC, INC.LINUX, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:INC,Malware:INC.LINUX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-155	Malicious File Transfer - INC, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:INC,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-156	Malicious File Transfer - INC, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:INC,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-157	Malicious File Transfer - INC, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:INC,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-158	Malicious File Transfer - INC, INC.LINUX, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:INC,Malware:INC.LINUX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-159	Malicious File Transfer - INC, INC.LINUX, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:INC,Malware:INC.LINUX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-160	Malicious File Transfer - INC, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:INC,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-161	Malicious File Transfer - INC, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:INC,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-162	Malicious File Transfer - INC, INC.LINUX, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:INC,Malware:INC.LINUX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-163	Malicious File Transfer - INC, Download, Variant #11	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:INC,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-164	Malicious File Transfer - INC, INC.LINUX, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:INC,Malware:INC.LINUX,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-165	Malicious File Transfer - INC, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:INC,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-166	Malicious File Transfer - INC, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:INC,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-167	Malicious File Transfer - CHERRYQUIRK, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CHERRYQUIRK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-168	Malicious File Transfer - CHERRYQUIRK, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CHERRYQUIRK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-169	Malicious File Transfer - UNC6452, CHERRYQUIRK, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6452,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CHERRYQUIRK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-170	Malicious File Transfer - UNC6452, CHERRYQUIRK, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6452,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CHERRYQUIRK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-171	Malicious File Transfer - UNC6452, CHERRYQUIRK, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6452,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CHERRYQUIRK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-172	Malicious File Transfer - AGENDA, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:AGENDA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-173	Malicious File Transfer - AGENDA, NESHTA, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:AGENDA,Malware:NESHTA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-174	Malicious File Transfer - AGENDA, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:AGENDA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-175	Malicious File Transfer - AGENDA, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:AGENDA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-176	Malicious File Transfer - AGENDA, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:AGENDA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-177	Malicious File Transfer - AGENDA, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:AGENDA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-178	Command and Control - AMADEY, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:AMADEY,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-179	Command and Control - BEACON.STAGER, Registration, Variant #1	ATT&CK:Command and Control,ATT&CK:M1030,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,ATT&CK:T1571,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:BEACON.STAGER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-180	Command and Control - BEACON.STAGER, METASPLOIT, Tasking, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:BEACON.STAGER,Malware:METASPLOIT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-182	Malicious File Transfer - AGENDA, Download, Variant #12	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:AGENDA,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-193	Malicious File Transfer - UNC2926, SILKAWEB, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2926,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SILKAWEB,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-195	Malicious File Transfer - LOUDWRITER, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:LOUDWRITER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-196	Malicious File Transfer - UNC5518, FAKETREFF, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5518,CAMP.24.061,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:FAKETREFF,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-200	Malicious File Transfer - UNC2465, SMOKEDHAM, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2465,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SMOKEDHAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-202	Malicious File Transfer - UNC5774, CORNFLAKE, CORNFLAKE.V2, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5774,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CORNFLAKE,Malware:CORNFLAKE.V2,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-203	Malicious File Transfer - UNC2465, SMOKEDHAM, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2465,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SMOKEDHAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-204	Phishing Email - Malicious Attachment, CROSSTRICK, 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,Control:Email,M-Trends 2026,Malware:CROSSTRICK,NIST:CM-7,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-205	Malicious File Transfer - UNC2465, SMOKEDHAM, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2465,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SMOKEDHAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-206	Phishing Email - Malicious Link, UNC4122, Variant #4	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC4122,Control:Email,M-Trends 2026,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-207	Malicious File Transfer - UNC2465, SMOKEDHAM, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2465,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SMOKEDHAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-208	Malicious File Transfer - UNC2465, SMOKEDHAM, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2465,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SMOKEDHAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-209	Malicious File Transfer - UNC2465, SMOKEDHAM, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2465,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SMOKEDHAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-210	Malicious File Transfer - UNC2465, SMOKEDHAM, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2465,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SMOKEDHAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-211	Phishing Email - Malicious Attachment, UNC2926, SILKAWEB, 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:UNC2926,Control:Email,M-Trends 2026,Malware:SILKAWEB,NIST:CM-7,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-213	Phishing Email - Malicious Attachment, UNC2926, 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:UNC2926,Control:Email,M-Trends 2026,NIST:CM-7,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-214	Phishing Email - Malicious Link, UNC4509, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC4509,Control:Email,M-Trends 2026,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-217	Malicious File Transfer - FIN6, SQUIDGATE, SQUIDSLEEP, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SQUIDGATE,Malware:SQUIDSLEEP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-222	Malicious File Transfer - RAZORBRAKE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:RAZORBRAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-223	Malicious File Transfer - UNC2165, COILCAGE, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:COILCAGE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-225	Malicious File Transfer - UNC2165, COILCAGE, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:COILCAGE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-227	Malicious File Transfer - UNC2165, COILCAGE, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,CAMP.24.024,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:COILCAGE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-228	Malicious File Transfer - UNC2165, COILCAGE, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:COILCAGE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-231	Malicious File Transfer - UNC2165, COILCAGE, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:COILCAGE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-233	Malicious File Transfer - VIDAR, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:VIDAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-234	Malicious File Transfer - RADTHIEF, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:RADTHIEF,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-235	Malicious File Transfer - UNC2165, COILCAGE, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:COILCAGE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-237	Malicious File Transfer - UNC2165, COILCAGE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:COILCAGE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-239	Malicious File Transfer - UNC2165, COILCAGE, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:COILCAGE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-240	Malicious File Transfer - UNC2165, NODEFRAME, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:NODEFRAME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-241	Malicious File Transfer - UNC2165, NODEFRAME, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:NODEFRAME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-242	Malicious File Transfer - FIN6, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,CAMP.23.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-244	Malicious File Transfer - FIN6, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-245	Malicious File Transfer - UNC2165, COILCAGE, RATTLEGRAB, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:COILCAGE,Malware:RATTLEGRAB,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-246	Malicious File Transfer - UNC5142, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5142,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-247	Malicious File Transfer - CROSSTRICK, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CROSSTRICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-248	Phishing Email - Malicious Link, UNC4122, Variant #2	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC4122,Control:Email,M-Trends 2026,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-250	Malicious File Transfer - UNC2165, NODEFRAME, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:NODEFRAME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-252	Malicious File Transfer - FIN6, BULLZLINK, Download, Variant #8	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:BULLZLINK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-253	Malicious File Transfer - UNC1543, UNC6490, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,Actor:UNC6490,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-254	Malicious File Transfer - UNC2165, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-256	Malicious File Transfer - FIN6, SQUIDGATE, SQUIDSLEEP, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SQUIDGATE,Malware:SQUIDSLEEP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-257	Malicious File Transfer - UNC2165, MYTHICAGENT, NODEFRAME, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:MYTHICAGENT,Malware:NODEFRAME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-258	Malicious File Transfer - FIN6, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-260	Malicious File Transfer - CROSSTRICK, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CROSSTRICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-261	Malicious File Transfer - UNC2165, NODEFRAME, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:NODEFRAME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-263	Malicious File Transfer - UNC2165, MYTHICAGENT, NODEFRAME, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:MYTHICAGENT,Malware:NODEFRAME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-265	Malicious File Transfer - FIN6, SQUIDGATE, SQUIDSLEEP, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SQUIDGATE,Malware:SQUIDSLEEP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-266	Malicious File Transfer - UNC1543, FAKEUPDATES, 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,M-Trends 2026,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-268	Malicious File Transfer - FIN6, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,CAMP.23.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-269	Malicious File Transfer - FIN6, BULLZLINK, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,CAMP.23.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:BULLZLINK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-270	Malicious File Transfer - CROSSTRICK, Download, Variant #7	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CROSSTRICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-271	Malicious File Transfer - UNC1543, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-272	Malicious File Transfer - FIN6, BULLZLINK, Download, Variant #6	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,CAMP.23.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:BULLZLINK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-273	Malicious File Transfer - FIN6, SQUIDGATE, SQUIDSLEEP, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SQUIDGATE,Malware:SQUIDSLEEP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-276	Malicious File Transfer - CROSSTRICK, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CROSSTRICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-278	Malicious File Transfer - UNC1543, FAKEUPDATES, 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,M-Trends 2026,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-279	Malicious File Transfer - UNC5142, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5142,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-283	Malicious File Transfer - UNC1543, FAKEUPDATES, 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,M-Trends 2026,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-285	Malicious File Transfer - FIN6, SQUIDGATE, SQUIDSLEEP, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SQUIDGATE,Malware:SQUIDSLEEP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-286	Malicious File Transfer - UNC5221, SPAWNSNARE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5221,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SPAWNSNARE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-287	Malicious File Transfer - UNC2165, COILCAGE, VIPERTUNNEL, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:COILCAGE,Malware:VIPERTUNNEL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-289	Malicious File Transfer - UNC4108, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC4108,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-290	Malicious File Transfer - UNC5221, SPAWNSNAIL, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5221,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SPAWNSNAIL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-293	Malicious File Transfer - UNC4108, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC4108,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-294	Malicious File Transfer - XWORM, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:XWORM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-297	Malicious File Transfer - XWORM, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:XWORM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-299	Malicious File Transfer - CROSSTRICK, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CROSSTRICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-301	Malicious File Transfer - CROSSTRICK, XWORM, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CROSSTRICK,Malware:XWORM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-302	Malicious File Transfer - RAZORBRAKE, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:RAZORBRAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-304	Malicious File Transfer - UNC6201, GRIMBOLT, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC6201,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:GRIMBOLT,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-306	Malicious File Transfer - UNC2565, GOOTLOADER, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2565,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:GOOTLOADER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-308	Malicious File Transfer - CROSSTRICK, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CROSSTRICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-309	Malicious File Transfer - CROSSTRICK, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CROSSTRICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-310	Malicious File Transfer - UNC2926, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2926,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-311	Malicious File Transfer - UNC5142, PALEBEAM, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5142,CAMP.24.045,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:PALEBEAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-312	Malicious File Transfer - VIDAR, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:VIDAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-313	Malicious File Transfer - VIDAR, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:VIDAR,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-314	Malicious File Transfer - UNC5142, PALEBEAM, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5142,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:PALEBEAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-320	Malicious File Transfer - CROSSTRICK, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CROSSTRICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-322	Malicious File Transfer - UNC5142, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5142,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-323	Malicious File Transfer - UNC5142, PALEBEAM, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC5142,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:PALEBEAM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-324	Malicious File Transfer - RAZORBRAKE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:RAZORBRAKE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-325	Malicious File Transfer - XWORM, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:XWORM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-326	Malicious File Transfer - CROSSTRICK, XWORM, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CROSSTRICK,Malware:XWORM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-328	Malicious File Transfer - RADTHIEF, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:RADTHIEF,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-329	Phishing Email - Malicious Link, UNC4122, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC4122,Control:Email,M-Trends 2026,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-331	Malicious File Transfer - RADTHIEF, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:RADTHIEF,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-332	Phishing Email - Malicious Link, UNC4122, Variant #3	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC4122,Control:Email,M-Trends 2026,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-334	Malicious File Transfer - UNC2926, SILKAWEB, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2926,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SILKAWEB,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-339	Phishing Email - Malicious Link, UNC2926, SILKAWEB, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC2926,Control:Email,M-Trends 2026,Malware:SILKAWEB,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-341	Malicious File Transfer - RADTHIEF, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:RADTHIEF,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-342	Phishing Email - Malicious Link, UNC5096, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1021,ATT&CK:M1031,ATT&CK:T1204.001,Actor:UNC5096,Control:Email,M-Trends 2026,OS:ANY,Src:External:Untrusted+Dst:Internal:Trusted
A108-346	Command and Control - UNC1543, FAKEUPDATES, Check-In, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1132,Actor:UNC1543,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:FAKEUPDATES,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-347	Malicious File Transfer - UNC4108, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC4108,CAMP.24.079,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-350	Command and Control - UNC1543, FAKEUPDATES, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,ATT&CK:T1132.001,Actor:UNC1543,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:FAKEUPDATES,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-359	Command and Control - FIN6, BULLZLINK, Check-In, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:FIN6,Control:IDS/IPS,Control:NGFW,Control:Proxy,Control:WAF,M-Trends 2026,Malware:BULLZLINK,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-360	Command and Control - UNC1543, FAKEUPDATES, Check-In, Variant #2	ATT&CK:Command and Control,ATT&CK:Exfiltration,ATT&CK:M1031,ATT&CK:M1057,ATT&CK:T1041,ATT&CK:T1071.001,Actor:UNC1543,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:FAKEUPDATES,NIST:AC-4,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-362	Malicious File Transfer - UNC2165, COILCAGE, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:COILCAGE,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-363	Command and Control - UNC1549, POLLREGISTER, Registration, 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,M-Trends 2026,Malware:POLLREGISTER,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-364	Command and Control - UNC2465, SMOKEDHAM, Communication, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1071.001,Actor:UNC2465,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SMOKEDHAM,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-374	Malicious File Transfer - UNC2165, COILCAGE, VIPERTUNNEL, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:COILCAGE,Malware:VIPERTUNNEL,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-376	Malicious File Transfer - CROSSTRICK, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CROSSTRICK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-377	Malicious File Transfer - CROSSTRICK, XWORM, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:CROSSTRICK,Malware:XWORM,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-380	Malicious File Transfer - FIN6, BULLZLINK, Download, Variant #9	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,CAMP.23.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:BULLZLINK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-381	Malicious File Transfer - FIN6, SQUIDGATE, SQUIDSLEEP, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:SQUIDGATE,Malware:SQUIDSLEEP,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-382	Malicious File Transfer - UNC2165, MYTHICAGENT, NODEFRAME, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC2165,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:MYTHICAGENT,Malware:NODEFRAME,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-383	Malicious File Transfer - FIN6, BULLZLINK, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:BULLZLINK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-384	Malicious File Transfer - FIN6, BULLZLINK, Download, Variant #3	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:BULLZLINK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-385	Malicious File Transfer - FIN6, BULLZLINK, Download, Variant #4	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:BULLZLINK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-386	Malicious File Transfer - FIN6, BULLZLINK, Download, Variant #5	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:BULLZLINK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-387	Malicious File Transfer - FIN6, BULLZLINK, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,CAMP.23.001,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:BULLZLINK,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-388	Malicious File Transfer - FIN6, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:FIN6,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-389	Malicious File Transfer - UNC1543, Download, Variant #1	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-390	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #2	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-391	Malicious File Transfer - UNC1543, FAKEUPDATES, 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,M-Trends 2026,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-392	Malicious File Transfer - UNC1543, FAKEUPDATES, 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,M-Trends 2026,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-393	Malicious File Transfer - UNC1543, FAKEUPDATES, 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,M-Trends 2026,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-394	Malicious File Transfer - UNC1543, FAKEUPDATES, 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,M-Trends 2026,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted
A108-395	Malicious File Transfer - UNC1543, FAKEUPDATES, Download, Variant #10	ATT&CK:Command and Control,ATT&CK:M1031,ATT&CK:T1105,Actor:UNC1543,CAMP.25.039,Control:IDS/IPS,Control:NGFW,Control:Proxy,M-Trends 2026,Malware:FAKEUPDATES,NIST:CM-7,OS:ANY,Src:Internal:Trusted+Dst:External:Untrusted

Host CLI Actions

VID	Name	Tags

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-191	Host CLI - Create Dnsclient Policy Registry Key, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.001,Actor:UNC6276,CWE:284,Control:Endpoint,M-Trends 2026,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:SYSTEM,Src:Internal:Trusted
A108-192	Host CLI - Discovery Via Obfuscated Powershell, Variant #1	ATT&CK:Execution,ATT&CK:M1026,ATT&CK:M1038,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1049,ATT&CK:T1059.001,Actor:UNC2465,Control:Endpoint,M-Trends 2026,NIST:CM-11,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-194	Host CLI - CRYTOX, Enable Wdigest Credential Caching, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1024,ATT&CK:Persistence,ATT&CK:T1112,Actor:UNC6276,CWE:15,CWE:732,Control:Endpoint,M-Trends 2026,Malware:CRYTOX,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:SYSTEM,Src:Internal:Trusted
A108-197	Host CLI - Decrypt Veeam Backup Credentials Using Powershell, Variant #1	ATT&CK:Credential Access,ATT&CK:M1017,ATT&CK:M1022,ATT&CK:M1027,ATT&CK:M1047,ATT&CK:T1552.001,Actor:UNC6361,CWE:259,CWE:522,CWE:798,Control:Endpoint,M-Trends 2026,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
A108-198	Host CLI - Modify /Etc/Motd File On Linux, Variant #1	ATT&CK:Impact,ATT&CK:M1053,ATT&CK:T1491.002,Actor:UNC6276,Control:Endpoint,M-Trends 2026,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-199	Host CLI - UNC6361, Active Directory User Discovery To File, Variant #1	ATT&CK:Discovery,ATT&CK:M1028,ATT&CK:T1087.002,Actor:UNC6361,Control:Endpoint,M-Trends 2026,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-201	Host CLI - Creates Rdp Connection History Registry Key, Variant #1	ATT&CK:Lateral Movement,ATT&CK:M1018,ATT&CK:M1026,ATT&CK:M1028,ATT&CK:M1030,ATT&CK:M1032,ATT&CK:M1035,ATT&CK:M1042,ATT&CK:M1047,ATT&CK:T1021.001,Actor:UNC6361,CWE:522,Control:Endpoint,M-Trends 2026,NIST:AC-17,NIST:CM-7,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
A108-215	Host CLI - Decrypt Application Data With Powershell Dpapi, Variant #1	ATT&CK:Credential Access,ATT&CK:M1027,ATT&CK:M1042,ATT&CK:M1051,ATT&CK:M1054,ATT&CK:T1555,Actor:UNC6361,Control:Endpoint,M-Trends 2026,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
A108-216	Host CLI - Create Kitty Registry Key, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1024,ATT&CK:Persistence,ATT&CK:T1112,Actor:UNC2465,CWE:15,CWE:732,Control:Endpoint,M-Trends 2026,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,RunAs:User,Src:Internal:Trusted
A108-221	Host CLI - Establishes Persistence Via Mtxoci Registry Key, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1024,ATT&CK:Persistence,ATT&CK:T1112,Actor:UNC2465,CWE:15,CWE:732,Control:Endpoint,M-Trends 2026,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:SYSTEM,Src:Internal:Trusted
A108-226	Host CLI - Establish Persistence With Wmic, Variant #1	ATT&CK:Execution,ATT&CK:M1018,ATT&CK:M1026,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1047,Actor:UNC2465,Control:Endpoint,M-Trends 2026,NIST:AC-17,NIST:CM-11,NIST:CM-7,NIST:IA-2,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-229	Host CLI - Create Scheduled Task For Execution, 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:UNC6276,Control:Endpoint,M-Trends 2026,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
A108-232	Host CLI - Obfuscated Powershell File Read, Variant #1	ATT&CK:Execution,ATT&CK:M1026,ATT&CK:M1038,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1049,ATT&CK:T1059.001,Actor:UNC2465,Control:Endpoint,M-Trends 2026,NIST:CM-11,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
A108-238	Host CLI - Copy Rundll32.Exe To Staging Directory, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1021,ATT&CK:M1022,ATT&CK:M1026,ATT&CK:M1037,ATT&CK:M1038,ATT&CK:M1042,ATT&CK:M1050,ATT&CK:T1218,Control:Endpoint,M-Trends 2026,NIST:CM-11,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
A108-300	Host CLI - UNC6201, Abuse Sudo For Privilege Escalation, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1026,ATT&CK:M1028,ATT&CK:Privilege Escalation,ATT&CK:T1548.003,Actor:UNC6201,CWE:306,Control:Endpoint,M-Trends 2026,NIST:AC-6,NIST:CM-11,NIST:CM-5,NIST:CM-7,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-321	Host CLI - Modify Esxi Local.Sh For Persistence, Variant #1	ATT&CK:M1022,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1037.004,Actor:UNC6201,Control:Endpoint,M-Trends 2026,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-335	Host CLI - Establish Netsh Port Proxy For C2, Variant #1	ATT&CK:Execution,ATT&CK:M1038,ATT&CK:T1059.003,Actor:UNC1549,Control:Endpoint,M-Trends 2026,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-336	Host CLI - Tomcat Web Shell Placement, Variant #1	ATT&CK:M1018,ATT&CK:M1042,ATT&CK:Persistence,ATT&CK:T1505.003,Actor:UNC6201,CWE:287,CWE:553,Control:Endpoint,M-Trends 2026,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-338	Host CLI - UNC5774, CORNFLAKE.V3.PHP, Establishes Persistence Via Registry Run Key, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:FIN6,Actor:UNC5774,Control:Endpoint,M-Trends 2026,Malware:CORNFLAKE.V3.PHP,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
A108-344	Host CLI - UNC2165, Outlook Signature Ntlm Credential Harvesting, Variant #1	ATT&CK:Credential Access,ATT&CK:M1027,ATT&CK:M1037,ATT&CK:T1187,Actor:UNC2165,CWE:200,CWE:522,CWE:601,Control:Endpoint,M-Trends 2026,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,RunAs:User,Src:Internal:Trusted
A108-353	Host CLI - BABUK, Add Smb Credentials With Cmdkey, Variant #1	ATT&CK:Credential Access,ATT&CK:M1042,ATT&CK:T1555.004,Actor:UNC2165,Control:Endpoint,M-Trends 2026,Malware:BABUK,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
A108-356	Host CLI - MEDUSA, Uac Bypass Via Fodhelper Com Abuse, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1026,ATT&CK:M1047,ATT&CK:M1051,ATT&CK:M1052,ATT&CK:Privilege Escalation,ATT&CK:T1548.002,Actor:FIN6,CWE:284,Control:Endpoint,M-Trends 2026,Malware:MEDUSA,NIST:AC-6,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
A108-357	Host CLI - Modify Msdtc Service To Run As Localsystem, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC2465,CWE:284,Control:Endpoint,M-Trends 2026,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:SYSTEM,Src:Internal:Trusted
A108-358	Host CLI - Persistence Via Registry Run Key, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC2465,Control:Endpoint,M-Trends 2026,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-361	Host CLI - UNC6361, AKIRA, Create Ransom Note, Variant #1	ATT&CK:Impact,ATT&CK:M1040,ATT&CK:M1053,ATT&CK:T1486,Actor:UNC6361,Control:Endpoint,M-Trends 2026,Malware:AKIRA,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
A108-365	Host CLI - Creates A Process Using Wmi, Variant #1	ATT&CK:Execution,ATT&CK:M1018,ATT&CK:M1026,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1047,Actor:UNC2165,Control:Endpoint,M-Trends 2026,NIST:AC-17,NIST:CM-11,NIST:CM-7,NIST:IA-2,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
A108-366	Host CLI - Disable Llmnr Via Registry, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1024,ATT&CK:Persistence,ATT&CK:T1112,Actor:UNC6276,CWE:15,CWE:732,Control:Endpoint,M-Trends 2026,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:SYSTEM,Src:Internal:Trusted
A108-367	Host CLI - Establishes Persistence Via 'Pubg Game' Registry Run Key, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC1543,Control:Endpoint,M-Trends 2026,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
A108-368	Host CLI - Executes Content From File Via Obfuscated Powershell, Variant #1	ATT&CK:Execution,ATT&CK:M1026,ATT&CK:M1038,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1049,ATT&CK:T1059.001,Actor:UNC2465,Control:Endpoint,M-Trends 2026,NIST:CM-11,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
A108-369	Host CLI - FAKEUPDATES, Steal Chrome Login Data, Variant #1	ATT&CK:Credential Access,ATT&CK:M1027,ATT&CK:T1555.003,Actor:UNC1543,CWE:522,Control:Endpoint,M-Trends 2026,Malware:FAKEUPDATES,OS:Windows Server:2016,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-370	Host CLI - NINTHBEE, Disable Mssql Service, Variant #1	ATT&CK:Impact,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:M1030,ATT&CK:T1489,Actor:UNC6276,Control:Endpoint,M-Trends 2026,Malware:NINTHBEE,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-371	Host CLI - UNC1543, BABUK, Adds Credentials With Cmdkey For Share Mounting, Variant #1	ATT&CK:Credential Access,ATT&CK:M1027,ATT&CK:M1051,ATT&CK:M1054,ATT&CK:T1555.005,Actor:UNC1543,Control:Endpoint,M-Trends 2026,Malware:BABUK,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
A108-372	Host CLI - UNC4108, NIGHTROPE, VOLTMARKER, Persistence Via 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:UNC1543,Actor:UNC4108,Control:Endpoint,M-Trends 2026,Malware:NIGHTROPE,Malware:VOLTMARKER,OS:Windows Server:2016,OS:Windows Server:2019,OS:Windows Server:2022,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-373	Host CLI - UNC5221, Placement Of Web Shell, Variant #1	ATT&CK:M1018,ATT&CK:M1042,ATT&CK:Persistence,ATT&CK:T1505.003,Actor:UNC5221,Actor:UNC6201,CWE:287,CWE:553,Control:Endpoint,M-Trends 2026,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
A108-375	Host CLI - UNC5774, CORNFLAKE.V3.PHP, Persistence Via Registry Run Key, Variant #1	ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1547.001,Actor:UNC2165,Actor:UNC5774,Control:Endpoint,M-Trends 2026,Malware:CORNFLAKE.V3.PHP,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

Protected Theater Actions

VID	Name	Tags
A108-108	Protected Theater - ADAPTAGENT, C2 Beacon, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Control:Endpoint,M-Trends 2026,Malware:ADAPTAGENT,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-153	Protected Theater - BEACON.STAGER, METASPLOIT, Drops A Randomly Named Payload, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Control:Endpoint,M-Trends 2026,Malware:BEACON.STAGER,Malware:METASPLOIT,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-183	Protected Theater - UNC6303, ADAPTAGENT, Network Connection, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6303,Control:Endpoint,M-Trends 2026,Malware:ADAPTAGENT,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A108-184	Protected Theater - AGENDA, NESHTA, To Drop Hconfig.Exe, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Control:Endpoint,M-Trends 2026,Malware:AGENDA,Malware:NESHTA,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-185	Protected Theater - ADAPTAGENT, Creates And Starts A Windows Service For Persistence, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,CWE:284,Control:Endpoint,M-Trends 2026,Malware:ADAPTAGENT,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-186	Protected Theater - AMADEY, SYSTEMBC.V2, Scheduled Task Persistence, 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,Control:Endpoint,M-Trends 2026,Malware:AMADEY,Malware:SYSTEMBC.V2,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-187	Protected Theater - BEACON, Executes Payload, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Control:Endpoint,M-Trends 2026,Malware:BEACON,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A108-188	Protected Theater - BEACON.STAGER, METASPLOIT, Execute Stager, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Control:Endpoint,M-Trends 2026,Malware:BEACON.STAGER,Malware:METASPLOIT,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A108-189	Protected Theater - AMADEY, LUMMAC.V2, SYSTEMBC.V2, Initiates Lummac Systembc C2, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Control:Endpoint,M-Trends 2026,Malware:AMADEY,Malware:LUMMAC.V2,Malware:SYSTEMBC.V2,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-190	Protected Theater - BEACON, Executes Payload To Trigger C2, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Control:Endpoint,M-Trends 2026,Malware:BEACON,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-218	Protected Theater - Disable Syslog Forwarding With Iptables, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1054,ATT&CK:T1562.006,Actor:UNC5221,Control:Endpoint,M-Trends 2026,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-219	Protected Theater - ECO2, UNC5267, Executes The Shell Script To Create A Configuration File, Variant #1	ATT&CK:Execution,ATT&CK:M1038,ATT&CK:T1059.004,Actor:UNC5267,Control:Endpoint,M-Trends 2026,NIST:CM-11,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-220	Protected Theater - FIN6, BULLZLINK, 'S Lnk Execution, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:FIN6,Control:Endpoint,M-Trends 2026,Malware:BULLZLINK,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-224	Protected Theater - FIN6, BULLZLINK, Downloader Establishing C2 Connection, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:FIN6,Control:Endpoint,M-Trends 2026,Malware:BULLZLINK,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-230	Protected Theater - FIN6, BULLZLINK, Executes Obfuscated Command To Run Inf Via Ie4Uinit.Exe, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1021,ATT&CK:M1022,ATT&CK:M1026,ATT&CK:M1037,ATT&CK:M1038,ATT&CK:M1042,ATT&CK:M1050,ATT&CK:T1218,Actor:FIN6,Control:Endpoint,M-Trends 2026,Malware:BULLZLINK,NIST:CM-11,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-236	Protected Theater - FIN6, BULLZLINK, Lnk Execution, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:FIN6,Control:Endpoint,M-Trends 2026,Malware:BULLZLINK,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-243	Protected Theater - FIN6, BULLZLINK, Triggers C2 Communication, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:FIN6,Control:Endpoint,M-Trends 2026,Malware:BULLZLINK,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-249	Protected Theater - FIN6, BULLZLINK, Uses An Obfuscated Command To Create A Malicious Inf File For Remote Code Execution, Variant #1	ATT&CK:Defense Evasion,ATT&CK:T1202,Actor:FIN6,Control:Endpoint,M-Trends 2026,Malware:BULLZLINK,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-251	Protected Theater - GOLDTOMB.STAGER, GOLDVEIN, Set Environment Variable For Payload Configuration, Variant #1	ATT&CK:Execution,ATT&CK:M1038,ATT&CK:T1129,Actor:FIN11,Actor:UNC2465,CWE:114,Control:Endpoint,M-Trends 2026,Malware:GOLDTOMB.STAGER,Malware:GOLDVEIN,NIST:CM-11,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-255	Protected Theater - Persistence Via Ccm Script Store, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1038,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1574.008,Actor:UNC1549,Control:Endpoint,M-Trends 2026,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-262	Protected Theater - Start Ssh Daemon On Non Standard Port, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1047,ATT&CK:T1562.007,Actor:UNC5807,Control:Endpoint,M-Trends 2026,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-264	Protected Theater - UNC1543, FAKEUPDATES, Create Service For Persistence, Variant #1	ATT&CK:M1018,ATT&CK:M1047,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1543.003,Actor:UNC1543,CWE:284,Control:Endpoint,M-Trends 2026,Malware:FAKEUPDATES,NIST:AC-3,NIST:AC-6,NIST:AU-2,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-267	Protected Theater - UNC1543, FAKEUPDATES, Execute Dropper, Variant #1	ATT&CK:Execution,ATT&CK:M1021,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:M1042,ATT&CK:T1059.007,Actor:UNC1543,Control:Endpoint,M-Trends 2026,Malware:FAKEUPDATES,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-274	Protected Theater - UNC1543, FAKEUPDATES, Executes The Javascript Dropper, Variant #1	ATT&CK:Execution,ATT&CK:M1021,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:M1042,ATT&CK:T1059.007,Actor:UNC1543,Control:Endpoint,M-Trends 2026,Malware:FAKEUPDATES,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-275	Protected Theater - UNC1543, FAKEUPDATES, Persistence Via 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:UNC1543,Control:Endpoint,M-Trends 2026,Malware:FAKEUPDATES,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-277	Protected Theater - UNC1549, CREDSTROKE, C2 Communication, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC1549,Control:Endpoint,M-Trends 2026,Malware:CREDSTROKE,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-280	Protected Theater - UNC1549, CREDSTROKE, Via Rundll32, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1050,ATT&CK:T1218.011,Actor:UNC1549,CWE:114,Control:Endpoint,M-Trends 2026,Malware:CREDSTROKE,NIST:CM-11,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-281	Protected Theater - UNC1549, POLLREGISTER, Executes Dropper Dll, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1050,ATT&CK:T1218.011,Actor:UNC1549,CWE:114,Control:Endpoint,M-Trends 2026,Malware:POLLREGISTER,NIST:CM-11,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-282	Protected Theater - UNC1549, TWOSTROKE, Beacons To C2 Server, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC1549,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-284	Protected Theater - UNC1549, TWOSTROKE, C2 Beacon, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC1549,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-288	Protected Theater - UNC1549, TWOSTROKE, C2 Communication, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC1549,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-291	Protected Theater - UNC1549, TWOSTROKE, Cabinet.Dll Execution, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1050,ATT&CK:T1218.011,Actor:UNC1549,CWE:114,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,NIST:CM-11,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-292	Protected Theater - UNC1549, TWOSTROKE, Configure Dll Sideload Via Migautoplay, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1013,ATT&CK:M1051,ATT&CK:Persistence,ATT&CK:Privilege Escalation,ATT&CK:T1574.002,Actor:UNC1549,CWE:114,CWE:706,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-295	Protected Theater - UNC1549, TWOSTROKE, Connects To A C2 Domain, 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:UNC1549,CWE:114,CWE:427,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-296	Protected Theater - UNC1549, TWOSTROKE, Dropper, 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:UNC1549,CWE:114,CWE:427,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-298	Protected Theater - UNC1549, TWOSTROKE, Drops A Decoy Pdf Document, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC1549,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-303	Protected Theater - UNC1549, TWOSTROKE, Drops Google Updater, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1022,ATT&CK:M1038,ATT&CK:M1045,ATT&CK:T1036.005,Actor:UNC1549,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-305	Protected Theater - UNC1549, TWOSTROKE, Execute Dll Via Rundll32, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1050,ATT&CK:T1218.011,Actor:UNC1549,CWE:114,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,NIST:CM-11,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-307	Protected Theater - UNC1549, TWOSTROKE, Executes Loader Via Hiring Portal.Exe, 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:UNC1549,CWE:114,CWE:427,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:User,Src:Internal:Trusted
A108-315	Protected Theater - UNC1549, TWOSTROKE, Executes To Connect To C2, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC1549,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-317	Protected Theater - UNC1549, TWOSTROKE, Executes To Connect To C2, Variant #2	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC1549,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-318	Protected Theater - UNC1549, TWOSTROKE, Execution Via Unbcl.Dll, 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:UNC1549,CWE:114,CWE:427,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-327	Protected Theater - UNC1549, TWOSTROKE, Hiring Portal Loader (Userenv.Dll), 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:UNC1549,CWE:114,CWE:427,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-333	Protected Theater - UNC1549, TWOSTROKE, Scheduled Task Masquerading As Google Update, 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,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-337	Protected Theater - UNC1549, TWOSTROKE, Via Scheduled Task ('Updater.Exe'), 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,Control:Endpoint,M-Trends 2026,Malware:TWOSTROKE,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-340	Protected Theater - UNC2465, SMOKEDHAM, Drops Dll Via Powershell, Variant #1	ATT&CK:Execution,ATT&CK:M1026,ATT&CK:M1038,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1049,ATT&CK:T1059.001,Actor:UNC2465,Control:Endpoint,M-Trends 2026,Malware:SMOKEDHAM,NIST:CM-11,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-343	Protected Theater - UNC2465, SMOKEDHAM, Powershell Dropper, Variant #1	ATT&CK:Defense Evasion,ATT&CK:Execution,ATT&CK:M1026,ATT&CK:M1038,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1049,ATT&CK:T1027.004,ATT&CK:T1059.001,Actor:UNC2465,Control:Endpoint,M-Trends 2026,Malware:SMOKEDHAM,NIST:CM-11,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-345	Protected Theater - UNC2465, SMOKEDHAM, Powershell Execution, Variant #1	ATT&CK:Execution,ATT&CK:M1026,ATT&CK:M1038,ATT&CK:M1042,ATT&CK:M1045,ATT&CK:M1049,ATT&CK:T1059.001,Actor:UNC2465,Control:Endpoint,M-Trends 2026,Malware:SMOKEDHAM,NIST:CM-11,OS:Windows:10,OS:Windows:11,RunAs:Admin,RunAs:SYSTEM,RunAs:User,Src:Internal:Trusted
A108-349	Protected Theater - UNC6201, GRIMBOLT, Executes And Checks For C2 Connection, Variant #1	ATT&CK:Execution,ATT&CK:M1017,ATT&CK:M1038,ATT&CK:M1040,ATT&CK:T1204.002,Actor:UNC6201,Control:Endpoint,M-Trends 2026,Malware:GRIMBOLT,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-351	Protected Theater - CRYTOX, MIMIKATZ, Modify Wdigest For Credential Dumping, Variant #1	ATT&CK:Credential Access,ATT&CK:M1026,ATT&CK:M1027,ATT&CK:M1047,ATT&CK:T1552.002,Actor:UNC6276,CWE:200,CWE:285,Control:Endpoint,M-Trends 2026,Malware:CRYTOX,Malware:MIMIKATZ,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

VID	Name	Tags
A108-352	Protected Theater - WHITERABBIT, Add Windows Defender Exclusions, Variant #1	ATT&CK:Defense Evasion,ATT&CK:M1018,ATT&CK:M1022,ATT&CK:M1024,ATT&CK:T1562.001,Actor:UNC5221,Actor:UNC5495,CWE:284,Control:Endpoint,M-Trends 2026,Malware:WHITERABBIT,NIST:AC-3,NIST:AC-6,NIST:AU-2,NIST:CM-5,OS:Windows Server:2016,OS:Windows:10,OS:Windows:11,RunAs:SYSTEM,Src:Internal:Trusted
A108-354	Protected Theater - Anti Forensics Using Sed, Variant #1	ATT&CK:Defense Evasion,ATT&CK:T1070.004,Actor:UNC5221,Control:Endpoint,M-Trends 2026,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted
A108-355	Protected Theater - Initiate Outbound Sftp Connection, Variant #1	ATT&CK:Execution,ATT&CK:M1038,ATT&CK:T1059.004,Actor:UNC5807,Control:Endpoint,M-Trends 2026,NIST:CM-11,OS:Linux:Ubuntu,RunAs:Root,RunAs:User,Src:Internal:Trusted

New Files

A total of 191 new files have been added to the File Library with this update. This includes 191 malicious files.

Malicious Files

File MD5	Tags
000afd08a4e889fe21a76d8d29ce3b96	Malware:NESHTA,Group:Validation
01f586016bbb1fce27ed0a6d6746f08b	Malware_Type:LAUNCHER,Group:Validation
0338905c708aae288cbc062e2f036691	Malware:KRABDRIP,Group:Validation,Malware_Type:DOWNLOADER
042542aec94432fc2cafe9a239144312	Malware:CROSSTRICK,Group:Validation,Malware_Type:DROPPER,Malware:XWORM
068433ef2fc83a88ff286be2876ac396	Malware:BULLZLINK,Malware_Type:DOWNLOADER,Group:Validation
0745aa7a66b6ae9095b588901fbf15ae	Malware:NODEFRAME,Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation,Malware:MYTHICAGENT
08759d9ea2712d693891c870bbebbde3	Malware:INC,Group:Validation,Malware_Type:RANSOMWARE
0d089e8e3842c30010b918bb9d1c4e08	Malware_Type:DOWNLOADER,Malware:BULLZLINK,Group:Validation
0ef874b5d77acb9f9f06fc0365f2e9e0	Malware_Type:BACKDOOR,Malware:ADAPTAGENT,Group:Validation
131abd79842e36faed42853252881d46	Malware:BULLZLINK,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
13672166042d63f7ff34f050ebb4b6e5	Malware:SMOKEDHAM,Malware_Type:DROPPER,Group:Validation
13ff3b65844595eb15292a87002ebe0b	Malware:NODEFRAME,Malware_Type:DROPPER_MEMORY_ONLY,Malware:MYTHICAGENT,Group:Validation
15408b74333bf4a6f4ac7d50cfcb843d	Malware:LUMMAC.V2,Group:Validation
1674e99668a20ce3ded7cfd9b3b73fe0	Group:Validation
17190c7e5163b5c115e3d470f568ee5f	Malware_Type:DOWNLOADER,Malware:VIDAR,Group:Validation
17743923ed195680bc116edbc5a17f67	Malware_Type:BACKDOOR,Malware:SQUIDSLEEP,Malware:SQUIDGATE,Group:Validation
18efd7ba2380b4b6ea13a7a36c0c77e2	Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation,Malware:COILCAGE
1a60a93c4b1c54d14ab260cb97749a1e	Group:Validation
1bb275319619856af055c3e292c4070a	Malware:AGENDA,Group:Validation
1d154306cb0824433bbf2674fac0e236	Malware_Type:DOWNLOADER,Group:Validation,Malware:KRABDRIP
1e3e29a85fc7fe89f3696facaa9db43c	Malware_Type:RANSOMWARE,Malware:REDBIKE,Group:Validation
209d2bdb17dddec96d907c72aa19cfa6	Group:Validation,Malware:BEACON
221173913fb34fd5978c706b2fc0edbc	Group:Validation,Malware:SQUIDSLEEP,Malware:SQUIDGATE,Malware_Type:BACKDOOR
225180b3366d190ece9f4b982af20857	Malware:KRABDRIP,Malware_Type:DOWNLOADER,Group:Validation
2459df4b9a46c72a4ba6603d246afc79	Malware:FAKEUPDATES,Group:Validation,Malware_Type:DOWNLOADER
24f1cc721eeeeb928016b872ccdf32d0	Malware:CROSSTRICK,Group:Validation,Malware_Type:DOWNLOADER
2502a72f1523efecbe0b52c8b7f5b637	Malware:JSPKIT,Group:Validation
25a81d4476e82cf9bfa9284aee09b436	Malware:VIPERTUNNEL,Group:Validation,Malware:COILCAGE
2654c08491a0f7c4a3dfc6282de5638b	Malware_Type:BACKDOOR,Malware:GRIMBOLT,Group:Validation
26852dac4e9c94dd24b40d23da94698f	Malware:SMOKEDHAM,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
26e2df6deb0609d1e86c7fa79608c8f7	Malware:NODEFRAME,Malware_Type:DROPPER_MEMORY_ONLY,Malware:MYTHICAGENT,Group:Validation
275dda19bc47a4f9b08e55dcff076252	Malware_Type:DOWNLOADER,Malware:FAKEUPDATES,Group:Validation
288a873227369a421dc7a4148c2d6613	Malware:SMOKEDHAM,Malware_Type:DROPPER,Group:Validation
29c7dcf9a9993db9f812362a0edd34cb	Malware:JSPKIT,Group:Validation
2afbb8ec4f11043122635951c374a761	Malware_Type:DOWNLOADER,Malware:RADTHIEF,Group:Validation
2bb853e2d71d314ffc5419ca3fc80a06	Group:Validation
2cd6334b20f474efbb3848ca1f34b3bc	Malware:COILCAGE,Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
2fc495605c5dd3af88db89aaf1543fa5	Malware:JSPKIT,Group:Validation
2fcde88eedb3414b9f0ce60fad83bf45	Group:Validation,Malware_Type:DOWNLOADER,Malware:KRABDRIP
3002c46792591d1bf8fe3ea1065b9496	Malware:CROSSTRICK,Group:Validation,Malware_Type:LAUNCHER
3016f81bddf5697bd23c5742a4e395e9	Malware:BULLZLINK,Malware_Type:DOWNLOADER,Group:Validation
35b41ecd23cc64020c5893a112f867ef	Malware_Type:DOWNLOADER,Group:Validation
35b59534d32de9ad2b8a839f2fd43ac2	Group:Validation,Malware:COILCAGE,Malware_Type:DROPPER_MEMORY_ONLY
36ee256294ad0c8b745844a730fb306a	Group:Validation,Malware:AMADEY,Malware:LUMMAC.V2,Malware_Type:DOWNLOADER,Malware:SYSTEMBC.V2
373f5ec571753bf2f2f435aef0382be8	Group:Validation,Malware_Type:DOWNLOADER,Malware:FAKETREFF
3a2997418eddac7083b06b4eae2cf413	Group:Validation
3a92a80962a5291ab839365aac79f94f	Malware:SILKAWEB,Malware_Type:DOWNLOADER,Group:Validation
3b4f0c8e44ae2b2d804b0e462c31ffd2	Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation,Malware:CROSSTRICK
3d019719b1192c7180419562c40e4b42	Malware:VIPERTUNNEL,Group:Validation,Malware:COILCAGE
3dcf695a66e4cbfae5bca8a66b792457	Malware:BULLZLINK,Malware_Type:DOWNLOADER,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
4029255b1ec03f2d0154d1dfd85bcbd5	Group:Validation
40cea72f1f84dc9686707c2428748eef	Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation,Malware:PALEBEAM
43ef3909c005037ccf6a29ef9df0ff79	Malware:JSPKIT,Group:Validation
43f420e2c4c81bc1511c8b323b5e24dd	Group:Validation,Malware:METASPLOIT,Malware:BEACON
44d377224eea6233764ecd7458bc9f5f	Malware_Type:DROPPER_MEMORY_ONLY,Malware:SMOKEDHAM,Group:Validation
471e2967c5b75492e246be8af1ba955f	Malware:SQUIDGATE,Group:Validation,Malware:SQUIDSLEEP,Malware_Type:BACKDOOR
47aff6fc736afa4f4d677a776fcad230	Malware:SILKAWEB,Group:Validation,Malware_Type:DOWNLOADER
4c458b976b583cda61aa8fa2827ab2cc	Malware:NODEFRAME,Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
4f24e034fe9a4d70dbf1e8e87dadca57	Malware:INC,Group:Validation
4fafddb01185d004e0ce986cb48e41c6	Malware:FAKEUPDATES,Malware_Type:DOWNLOADER,Group:Validation
52a62aaf5fb24eb66fc6580781659b53	Malware:NESHTA,Group:Validation
55152cc5af458a67e7b03d9b9439177f	Malware:SMOKEDHAM,Group:Validation
58f82ce8f15dcf5d334bf1b85534b3f1	Malware_Type:DOWNLOADER,Group:Validation,Malware:KRABDRIP
5aa9bf8620b1540f8696bf4158b49f36	Malware:NESHTA,Group:Validation
5b8b47c66901701c6ff6e084cb691f3f	Group:Validation
5c56da1927a0c85be657e863a2675822	Group:Validation
5c6a11c3061601d3be3462dd652e35ba	Malware:AGENDA,Group:Validation
5d6c1e24aee92ac63da0b1d7bbdf8d20	Group:Validation,Malware_Type:DROPPER,Malware:RAZORBRAKE
5e254632570183d3d9caea65bd6553aa	Malware:RADTHIEF,Group:Validation
61203caa2d53c64ce2cc517cb872311f	Malware_Type:DOWNLOADER,Malware:FAKEUPDATES,Group:Validation
6238e3fb2619f467c76f5d14e674c702	Group:Validation,Malware:AGENDA
630ad52d53b9c4f2b571d3b7c39d6eb7	Malware_Type:WEBSHELL,Malware:JSPKIT,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
63c8c7e27d0e1f148a14308eb733fceb	Malware_Type:DOWNLOADER,Group:Validation,Malware:BULLZLINK
63d1f533b8c5cd1639c189b07554b646	Group:Validation,Malware:INC
6431c8512b3221ec180478cb260da419	Malware:AGENDA,Group:Validation
648a0ae00b8946b298c7bd8b40ab3819	Group:Validation
66575cc1df33e40a47fe00abdc067fe5	Malware_Type:DOWNLOADER,Malware:CHERRYQUIRK,Group:Validation
66a2e864a54ca8077a89d4f72926b442	Group:Validation,Malware:CROSSTRICK,Malware_Type:DOWNLOADER
68a37177f8ab0fa25fc0385d057050a6	Group:Validation
6922606513cb616bb1da91e127813c59	Malware_Type:DOWNLOADER,Malware:FAKEUPDATES,Group:Validation
6936d7c46d2e2716fc19606d70f22d37	Group:Validation,Malware_Type:BACKDOOR,Malware:TWOSTROKE
6943e1be99c85953c565a1b22668db05	Group:Validation,Malware:INC
695dc51d26000878eb826d5524e5725e	Malware:BULLZLINK,Malware_Type:DOWNLOADER,Group:Validation
6b2a7eee6d049a8cb59692e6f47b0434	Group:Validation
6d1b444c6e3613657a800b45cfb8929c	Malware:FAKEUPDATES,Malware_Type:DOWNLOADER,Group:Validation
6d9648c1b7c22fa01db6efdc46f23611	Malware:SYSTEMBC,Malware_Type:TUNNELER,Malware:SYSTEMBC.PERL,Group:Validation
6e01ef1367ea81994578526b3bd331d6	Malware:SPAWNSNARE,Group:Validation,Malware_Type:UTILITY
6ee77a2dc19f4b96f61356a1efa2ddb8	Group:Validation
6f0343f0346d7ba701a1df796c9e10ca	Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation,Malware:COILCAGE
6fae7fbdf0231598e2b4aa8bb9b1c248	Malware_Type:DOWNLOADER,Group:Validation,Malware:VIDAR
708450f590eaf23e869080d09ed14e01	Malware:KRABDRIP,Malware_Type:DOWNLOADER,Group:Validation
715b2057e0f634912131f60e6cea158e	Malware_Type:DOWNLOADER,Malware:CHERRYQUIRK,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
721a103a640bde9d38aec9ea5f03eb98	Malware:SMOKEDHAM,Group:Validation,Malware_Type:DROPPER_MEMORY_ONLY
7462dd0c3e7d93b0e773da53b82a0882	Malware_Type:DOWNLOADER,Malware:FAKEUPDATES,Group:Validation
772b766281f54f80d767beef1eb74438	Malware:FAKEUPDATES,Group:Validation,Malware_Type:DOWNLOADER
780a6443312a97c4c04955d21f767bd1	Malware_Type:RANSOMWARE,Malware:REDBIKE.LINUX,Group:Validation
7d190efc6f17869ee01cf667c90d0211	Group:Validation,Malware:KRABDRIP,Malware_Type:DOWNLOADER
7e23f2323298ebd280e3fd2dea5fdab5	Group:Validation,Malware:AGENDA
80919bac16a22d74f914480874790f68	Malware:BEACON,Malware_Type:BACKDOOR,Group:Validation
80b2923e4e1cefa61521f44695262b85	Group:Validation
81ef0c1c9346bc6b0bcc9d100e76fdcf	Group:Validation
83d5fd9e89d2a49034f02f7be28eb598	Group:Validation
842fad5b26663ab4c3f01ff3e5d518e9	Malware:XWORM,Group:Validation,Malware_Type:DROPPER_MEMORY_ONLY,Malware:CROSSTRICK
843bd77cedd6003db9641f7ad07878c4	Malware_Type:BACKDOOR,Malware:XWORM,Group:Validation
851c6b405e024bfa765e48c8fa24c30b	Malware:INC,Group:Validation
87bb271276d17f043a018dcce6525e69	Group:Validation
881f9a4464b4fbec4799abefc8c0b421	Group:Validation,Malware_Type:DOWNLOADER,Malware:KRABDRIP
885c7b083023061b9cbb89bd44d15fcc	Malware:JSPKIT,Group:Validation
8a3d345edd1b359a5db24ff84b43d0de	Group:Validation,Malware:SQUIDSLEEP,Malware:SQUIDGATE,Malware_Type:BACKDOOR
8a49c4ba1731a17138bd6f2d3b962a60	Group:Validation,Malware_Type:BACKDOOR,Malware:XWORM
8c00feb53759f3ee4f3cdce0c70b431c	Group:Validation,Malware:INC.LINUX
8c5af430cb5eb86cc6644ea339d9e344	Group:Validation,Malware:COILCAGE,Malware_Type:DROPPER_MEMORY_ONLY
8c7bfe55f66beac56aab2748d9751795	Malware:FAKEUPDATES,Malware_Type:DOWNLOADER,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
8c8681e805e0ae7a7d1a609efc000c84	Malware:KRABDRIP,Malware_Type:DOWNLOADER,Group:Validation
8d2366f46188c5aa33c2a8bb2e4f8e7e	Group:Validation
8e39272825474579def1fed0ce02e712	Malware:BULLZLINK,Malware_Type:DOWNLOADER,Group:Validation
90259b42466d2256ea0b9956a51af389	Group:Validation,Malware:SMOKEDHAM
908a5cc9345bdd81e078c8b6145092e9	Malware:FAKEUPDATES,Group:Validation,Malware_Type:DOWNLOADER
9635c1576c885233f07fe1aab9bd660f	Malware_Type:DROPPER,Group:Validation,Malware:CHERRYQUIRK
963fe5f745ea94f8436abfb9ea6cb042	Malware:PALEBEAM,Malware_Type:DOWNLOADER,Group:Validation
96da4c9b10159e9a9a38a2e6aacbc984	Malware:RADTHIEF,Group:Validation
98ff64416ca81ce3926e59b0b094c7cf	Group:Validation
9a2d2aca0724d6b68b910d0024d4811a	Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation,Malware:RATTLEGRAB,Malware:COILCAGE
9d977438170744a36fb0bf9a57eda020	Malware:NODEFRAME,Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
9e81962848dd07baa3c615bf8feb06bf	Malware:CHERRYQUIRK,Group:Validation,Malware_Type:DOWNLOADER
9f057f46ead367cbd0abd35715626ba3	Group:Validation,Malware_Type:DOWNLOADER,Malware:CROSSTRICK
a0536969d73946775b6f51a3475909a1	Group:Validation
a06a149e3e974e418dc376e34748e3b8	Malware:NODEFRAME,Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
a39798f77e3aa06202d81e57b5d81acf	Group:Validation
a4ac7c7ed8292e9f8ed8c4e18e195736	Malware:JSPKIT,Group:Validation
a58728a10fe9b1147c5d627ac880db1e	Group:Validation,Malware:AMADEY,Malware_Type:DOWNLOADER,Malware:SYSTEMBC.V2
a5d8608c6bb4874880db60edcd90bbc6	Malware:AGENDA,Group:Validation
a6c9fe522b10b8aaab2e8ff5174e9cfa	Malware_Type:DROPPER_MEMORY_ONLY,Malware:COILCAGE,Group:Validation
a71b5881a9fd9b68eb05ebffbef2a618	Group:Validation,Malware:RADTHIEF

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
aac609cc11223d5b9a928de17b571ee8	Malware:COILCAGE,Group:Validation
aed7eef30dbb0e95290b82d8cdb80cef	Malware_Type:DOWNLOADER,Malware:KRABDRIP,Group:Validation
b384b974a0c542972aafeaf158423b83	Malware_Type:DOWNLOADER,Malware:KRABDRIP,Group:Validation
b3fe133b263e2bb19952fff7655bda86	Malware:FAKEUPDATES,Malware_Type:DOWNLOADER,Group:Validation
b6905066d0c6c24e04412367ef9ece94	Group:Validation,Malware_Type:DOWNLOADER,Malware:LOUDWRITER
b88ecabbb66029e2306aa91926a77eda	Group:Validation
b8f8130e99f922353d20d7cf48fdd734	Malware:CROSSTRICK,Group:Validation,Malware_Type:DROPPER_MEMORY_ONLY
bc8e8210e20a8dfeb04e8ad9ccc6fe9b	Group:Validation,Malware:AGENDA
bd80a35a57eb62d492ffdea215e3c346	Group:Validation
be22cb1170e2126b8809b7a6bf7d59ee	Group:Validation,Malware_Type:BACKDOOR,Malware:ADAPTAGENT
be808b641fb2d5498d8cb9d15a7c25af	Malware_Type:DROPPER,Group:Validation,Malware:RAZORBRAKE
be93b8514d7ca3733ffef38c966f4164	Group:Validation
bee36e45b0b3a9395a160b0bd16f015b	Group:Validation
bf0619b30a20af0504eae0fb61315454	Malware_Type:BACKDOOR,Malware:XWORM,Group:Validation
bf262e47207abca33fdb2d15d060f3f4	Malware:AGENDA,Group:Validation
bffc4bd2a7b56b02a7cdf85dd0189163	Group:Validation,Malware:CROSSTRICK,Malware_Type:DOWNLOADER
c392262fa86c390a20b998970639a51c	Malware:BRICKSTORM,Malware_Type:BACKDOOR,Group:Validation
c6991024d7107c592c6795a6a16ab6ed	Malware:REDBIKE,Group:Validation
c74c4e67a8e5847a44598ba6be51a6f8	Malware:JSPKIT,Group:Validation
cc230b816e851d87450e4db5b44c3c43	Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation,Malware:PALEBEAM
cdfac6e469556c49ec6e689fcf162861	Malware_Type:DROPPER,Malware:CHERRYQUIRK,Group:Validation

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
cff770423b66ff04c9c7d2255e524d9b	Group:Validation,Malware:METASPLOIT,Malware:BEACON
d22b10ac75dd7344724429471f05f98c	Group:Validation,Malware:INC.LINUX
d285d69b08632f030bc48acac8a2f5b5	Malware:BULLZLINK,Malware_Type:DOWNLOADER,Group:Validation
d3c37b7baaf5a2b754c9823f9cdde23e	Group:Validation,Malware:JSPKIT
d88907d30137e95f804548d96f2be20a	Group:Validation,Malware_Type:BACKDOOR,Malware:ADAPTAGENT
da09945e0948833f8c0b5fb97e78f6c9	Malware:INC,Group:Validation
da8b6699a51a2c4f8639f89faa1fe06c	Malware_Type:DOWNLOADER,Malware:CROSSTRICK,Group:Validation
dd475afd948cc22caa2a0f934d0aec52	Malware:AGENDA,Group:Validation
de4d1dd2e686c65a64bfdc1a9a51d9fe	Group:Validation,Malware_Type:DROPPER_MEMORY_ONLY,Malware:RAZORBRAKE
df9cfd04d8cda6df8f7263af54f9e5b1	Malware:NODEFRAME,Group:Validation,Malware_Type:DROPPER_MEMORY_ONLY
e0a17b8a3149ff065637879c5cb1fedd	Group:Validation,Malware:SMOKEDHAM
e0d8a0f8203b7a5ec2dd214d07c0b3f5	Malware:FAKEUPDATES,Group:Validation,Malware_Type:DOWNLOADER
e0ee713e5ca1b2e4761d32f671acda57	Malware_Type:DOWNLOADER,Malware:BULLZLINK,Group:Validation
e16c8c285b1d537be5fe32e93247c282	Malware:TWOSTROKE,Malware_Type:BACKDOOR,Group:Validation
e186176bbd1c8c5efdf1d26bee937668	Malware_Type:DROPPER_MEMORY_ONLY,Malware:XWORM,Group:Validation,Malware:CROSSTRICK
e3e4d2584e05d0a72c2b24723c468f96	Malware:BULLZLINK,Group:Validation,Malware_Type:DOWNLOADER
e566a30ae99c65f007514204143c64b5	Group:Validation,Malware:SMOKEDHAM
e631a4b81d011301edaef75b80de0cb2	Group:Validation,Malware:INC
e7387b926610a7f23177f2182cce0b9f	Malware:BEACON,Malware_Type:BACKDOOR,Group:Validation
e7d24813535f74187db31d4114f607a1	Malware_Type:BACKDOOR,Malware:SPAWNSNAIL,Group:Validation
e83a67a484b56684f1c7cc8cb0f071e4	Group:Validation,Malware_Type:DOWNLOADER,Malware:KRABDRIP

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

File MD5	Tags
e8dd3e343923ecc8f0ca78be840da2e2	Group:Validation,Malware_Type:BACKDOOR,Malware:SQUIDSLEEP,Malware:SQUIDGATE
e94affb98148fc4e0cfb9a486bb37160	Malware_Type:DATA_MINER,Malware:VIDAR,Group:Validation
ea1f8794c73b26724314e5356f1f4128	Malware:NESHTA,Malware:AGENDA,Group:Validation
ea937d71ab96f033f9d7af4ebba2dc52	Malware:CORNFLAKE.V2,Group:Validation,Malware_Type:DOWNLOADER
ecf43db2a281991f69063448353fa731	Malware:COILCAGE,Group:Validation,Malware_Type:DROPPER_MEMORY_ONLY
ed5f57ea54fcdec528fb28e2c4fa90ba	Group:Validation,Malware:GOOTLOADER,Malware_Type:DOWNLOADER
eed034535df3a7ad94fca08102af9dfd	Malware:KRABDRIP,Malware_Type:DOWNLOADER,Group:Validation
f1dffeea8e34d7803aa669878863a658	Group:Validation,Malware:SYSTEMBC.V2,Malware_Type:TUNNELER
f3f6b4ac227e7f5432fb5c805d629c4d	Malware_Type:DOWNLOADER,Malware:CROSSTRICK,Group:Validation
f78742cce17a523ac75299382575fa26	Malware:BULLZLINK,Malware_Type:DOWNLOADER,Group:Validation
f907e28d47bf17cd4d534fca28a38d87	Group:Validation,Malware_Type:DOWNLOADER,Malware:KRABDRIP
fa2f68aad2d0feb8258b6911afc4c8b9	Group:Validation,Malware_Type:BACKDOOR,Malware:ADAPTAGENT
fd298cc6e4828b95473ed6f5d2af3113	Malware:AGENDA,Group:Validation
fd97d2574e631f5b362509d5df7624f6	Malware:COILCAGE,Malware_Type:DROPPER_MEMORY_ONLY,Group:Validation
ff05e87fcc54065f1cc9cbcd75e23e03	Malware_Type:BACKDOOR,Group:Validation,Malware:SQUIDSLEEP,Malware:SQUIDGATE

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 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

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

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.