

AdversaryGraph

Threat Intelligence Analysis Report

Analysis Metadata

Provider:	deterministic
Model:	tshark-evidence-v3
Domain:	enterprise-attack
Session ID:	869e7fd1-f976-40e4-affa-f9960f431cf8
Review state:	draft
Generated:	2026-09-19 12:41 UTC

DRAFT ASSESSMENT - This report revision is not promoted and must not be treated as authoritative intelligence.

Key Findings

0 Techniques accepted	0 Group similarity leads	N/A Top group similarity	0 High-confidence findings
---	--	--	--

Executive Summary

Decoded 9221 packets across 66 IP endpoints and 263 transport flows. Observed 199 DNS events, 58 HTTP requests, 105 TLS ClientHello events, and 45 exported HTTP object(s). Deterministic rules produced 9 finding(s): 0 high, 2 medium, and 7 low. Findings are evidence-bound candidates and require analyst review; encrypted payload contents remain unavailable.

Review Gate Assessment

State: draft
Profile: internal_ir
Revision: 1
Policy: report-review-policy-v1.0
Coverage: 40000 / 40939 characters
Promotion ready: No

#	Gate	Machine	Analyst	Reason
1	Source provenance	warning	pending	
2	Publication date	fail	pending	
3	Procedure relevance	warning	pending	
4	Procedure-level claim	fail	pending	
5	Actor identification	warning	pending	

Promotion blockers

- source_analysis_coverage_incomplete
- gate_pending:source_provenance
- gate_pending:publication_date
- gate_pending:procedure_relevance
- gate_pending:procedure_level_claim
- gate_pending:actor_identification
- claims_unresolved:201
- accepted_procedure_claim_required
- accepted_publication_date_claim_required

Machine and AI findings are advisory. Only authenticated analyst gate decisions and accepted, source-bound claims determine promotion readiness.

Packet Evidence Appendix

Observed packet data and rule candidates. This appendix does not approve ATT&CK mappings, maliciousness, or actor attribution.

AdversaryGraph Deterministic PCAP Analysis

Source: 2021-09-10-traffic-analysis-exercise.pcap

Capture SHA-256: `a9576008f7fd634740253a52b2937a205cd214cdde09f6924f0921b8e266dd12`

Semantic result SHA-256: `ce8b10a4ba7a6615d2c58f5895ecb69dca768d904402026068da26b4ef7db5ed`

Analyzer manifest SHA-256: `ee952aeb7cdc6958f4ae5178c54c274a1e4f0aec4d42f3bdb95baaff063b3dde`

Executive summary

Decoded 9221 packets across 66 IP endpoints and 263 transport flows. Observed 199 DNS events, 58 HTTP requests, 105 TLS ClientHello events, and 45 exported HTTP object(s). Deterministic rules produced 9 finding(s): 0 high, 2 medium, and 7 low. Findings are evidence-bound candidates and require analyst review; encrypted payload contents remain unavailable.

Capture facts

- Packets: 9221
- Duration: 4609.2884 seconds
- Captured bytes: 6032490
- Endpoints: 66
- Flows: 263

Deterministic findings

MEDIUM \u2014 Script, archive, or executable transfer candidate

HTTP metadata names a script, archive, or executable. This is a transfer candidate, not proof of file type, execution, or malicious intent; legitimate updates use the same formats.

Rule: `script-or-executable-transfer@pcap-rules-v3`; confidence: 0.86; evidence: frame 4193 / TCP stream 100, frame 4198 / TCP stream 100, frame 4200 / TCP stream 100, frame 6404 / TCP stream 100.

Metrics: `{ "content_type": "application/octet-stream", "declared_body_bytes": 1048578, "destination": "10.9.10.102", "response_count": 2, "source": "2.3.1.237.216", "uri": "/d/msdownload/update/software/defu/2021/09/am_delta_patch_1.349.439.0_dcf977cccce1b58289d270f71f8151b3acc1566b.exe" }

MEDIUM \u2014 Script, archive, or executable transfer candidate

HTTP metadata names a script, archive, or executable. This is a transfer candidate, not proof of file type, execution, or malicious intent; legitimate updates use the same formats.

Rule: `script-or-executable-transfer@pcap-rules-v3`; confidence: 0.86; evidence: frame 4195 / TCP stream 101, frame 4199 / TCP stream 101, frame 4201 / TCP stream 101, frame 6356 / TCP stream 101, frame 6371 / TCP stream 101.

Metrics: `{ "content_type": "application/octet-stream", "declared_body_bytes": 1970634, "destination": "10.9.10.102", "response_count": 3, "source": "2.3.1.237.225", "uri": "/d/msdownload/update/software/defu/2021/09/am_delta_patch_1.349.439.0_dcf977cccce1b58289d270f71f8151b3acc1566b.exe" }

LOW \u2014 Repeated unsuccessful DNS resolution

Repeated NXDOMAIN responses may indicate a dead domain, misconfiguration, retrying software, or malicious fallback. They do not establish a domain-generation algorithm.

Rule: `repeated-nxdomain@pcap-rules-v3`; confidence: 0.5; evidence: frame 19, frame 64, frame 134, frame 168, frame 7624.

Metrics: `{ "domain": "wpad.angrypoutine.com", "response_count": 12, "source": "10.9.10.102" }

LOW \u2014 Directory-service protocol activity

Directory protocol operations were decoded. Normal Windows logon uses these protocols; activity alone does not establish discovery, credential

theft, or DCSync.

Rule: `directory-service-activity@pcap-rules-v3`; confidence: 0.95; evidence: frame 389 / TCP stream 15, frame 398 / TCP stream 15, frame 404 / TCP stream 15, frame 417 / TCP stream 15, frame 2059 / TCP stream 67.

Metrics: `{"destination":"10.9.10.9","event\_count":25,"operation\_numbers":["0","1","12"],"protocol":"drsuapi","source":"10.9.10.102"}`

LOW \u2014 Directory-service protocol activity

Directory protocol operations were decoded. Normal Windows logon uses these protocols; activity alone does not establish discovery, credential theft, or DCSync.

Rule: `directory-service-activity@pcap-rules-v3`; confidence: 0.95; evidence: frame 80 / TCP stream 1, frame 83 / TCP stream 1, frame 478 / TCP stream 22, frame 483 / TCP stream 22, frame 486 / TCP stream 22.

Metrics: `{"destination":"10.9.10.9","event\_count":50,"operation\_numbers":["0","2","3"],"protocol":"ldap","source":"10.9.10.102"}`

LOW \u2014 Directory-service protocol activity

Directory protocol operations were decoded. Normal Windows logon uses these protocols; activity alone does not establish discovery, credential theft, or DCSync.

Rule: `directory-service-activity@pcap-rules-v3`; confidence: 0.95; evidence: frame 440 / TCP stream 19, frame 442 / TCP stream 19, frame 444 / TCP stream 19, frame 446 / TCP stream 19, frame 448 / TCP stream 19.

Metrics: `{"destination":"10.9.10.9","event\_count":57,"operation\_numbers":["1","16","17","18","19","20","25","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"10.9.10.102"}`

LOW \u2014 Directory-service protocol activity

Directory protocol operations were decoded. Normal Windows logon uses these protocols; activity alone does not establish discovery, credential theft, or DCSync.

Rule: `directory-service-activity@pcap-rules-v3`; confidence: 0.95; evidence: frame 391 / TCP stream 15, frame 401 / TCP stream 15, frame 406 / TCP stream 15, frame 418 / TCP stream 15, frame 2060 / TCP stream 67.

Metrics: `{"destination":"10.9.10.102","event\_count":25,"operation\_numbers":["0","1","12"],"protocol":"drsuapi","source":"10.9.10.9"}`

LOW \u2014 Directory-service protocol activity

Directory protocol operations were decoded. Normal Windows logon uses these protocols; activity alone does not establish discovery, credential theft, or DCSync.

Rule: `directory-service-activity@pcap-rules-v3`; confidence: 0.95; evidence: frame 82 / TCP stream 1, frame 480 / TCP stream 22, frame 485 / TCP stream 22, frame 487 / TCP stream 22, frame 495 / TCP stream 23.

Metrics: `{"destination":"10.9.10.102","event\_count":39,"operation\_numbers":["1","4,19,19,19,5","4,5","5"],"protocol":"ldap","source":"10.9.10.9"}`

LOW \u2014 Directory-service protocol activity

Directory protocol operations were decoded. Normal Windows logon uses these protocols; activity alone does not establish discovery, credential theft, or DCSync.

Rule: `directory-service-activity@pcap-rules-v3`; confidence: 0.95; evidence: frame 441 / TCP stream 19, frame 443 / TCP stream 19, frame 445 / TCP stream 19, frame 447 / TCP stream 19, frame 449 / TCP stream 19.

Metrics: `{"destination":"10.9.10.102","event\_count":57,"operation\_numbers":["1","16","17","18","19","20","25","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"10.9.10.9"}`

ATT&CK candidates

- T1105 Ingress Tool Transfer (command-and-control), confidence=0.8, status=suggested; basis=versioned-deterministic-rule.

Identities

- account: `hobart.gunnarsson`; client IPs: 10.9.10.102; frames: 300, 311, 315, 332, 341
- full-name: `Hobart Gunnarsson`; client IPs: 10.9.10.102; frames: 455
- hostname: `DESKTOP-KKITB6Q`; client IPs: 10.9.10.102, 169.254.181.227; frames: 1, 3, 5, 6, 9
- netbios-group: `ANGRYPOUTINE`; client IPs: unbound subject; frames: 7, 8, 11, 35, 38

IOC and artifact candidates

- domain: `68091d435f184f9c8d6273bdb538ff4b.clo.footprintdns.com`; roles: dns-query, tls-sni
- domain: `a-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `am2prdapp01-canary.cloudapp.net`; roles: dns-cname
- domain: `angrypoutine-dc.angrypoutine.com`; roles: dns-query
- domain: `angrypoutine.com`; roles: dns-query
- domain: `api.msn.com`; roles: dns-query, tls-sni
- domain: `au.download.windowsupdate.com`; roles: dns-query, http-host
- domain: `bing.com`; roles: tls-sni
- domain: `cdn.onenote.net`; roles: dns-query, tls-sni
- domain: `client.wns.windows.com`; roles: tls-sni
- domain: `cp601.prod.do.dsp.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `ctldl.windowsupdate.com`; roles: dns-query, http-host
- domain: `desktop-kkitb6q.angrypoutine.com`; roles: dns-query
- domain: `desktop-muyeyv7.angrypoutine.com`; roles: dns-query
- domain: `dns.msftncsi.com`; roles: dns-query
- domain: `download.windowsupdate.com`; roles: dns-query, http-host
- domain: `evoke-windowsservices-tas.msedge.net`; roles: dns-query, tls-sni
- domain: `f005cab8a8840abf6ab35152a071b205.clo.footprintdns.com`; roles: dns-query, tls-sni
- domain: `fe2cr.update.microsoft.com`; roles: dns-query, tls-sni
- domain: `fe2cr.update.microsoft.com.akadns.net`; roles: dns-cname
- domain: `fe3cr.delivery.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `fp-afd.azureedge.us`; roles: dns-query, tls-sni
- domain: `fp-afd.azurefd.us`; roles: dns-query, tls-sni
- domain: `fp-vs-nocache.azureedge.net`; roles: dns-query, tls-sni
- domain: `fp.msedge.net`; roles: dns-query, tls-sni
- domain: `fs.microsoft.com`; roles: dns-query, tls-sni
- domain: `gameplayapi.intel.com`; roles: dns-query, tls-sni
- domain: `geo.prod.do.dsp.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `k-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `kv601.prod.do.dsp.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `login.live.com`; roles: dns-query, tls-sni
- domain: `microsoft.com`; roles: dns-query, tls-sni
- domain: `moiafdazure.clo.footprintdns.com`; roles: dns-query, tls-sni
- domain: `myexternalip.com`; roles: dns-query, tls-sni
- domain: `nexus.officeapps.live.com`; roles: dns-query, tls-sni
- domain: `nexusrules.officeapps.live.com`; roles: dns-query, tls-sni
- domain: `office15client.microsoft.com`; roles: dns-query
- domain: `prod-w.nexus.live.com.akadns.net`; roles: dns-cname
- domain: `prod.nexusrules.live.com.akadns.net`; roles: dns-cname
- domain: `q-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `s-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `settings-win.data.microsoft.com`; roles: dns-query, tls-sni
- domain: `settingsfd-geo.trafficmanager.net`; roles: dns-cname
- domain: `simpsonssavings.com`; roles: dns-query, http-host
- domain: `slscr.update.microsoft.com`; roles: dns-query, tls-sni
- domain: `spo-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `store-images.s-microsoft.com`; roles: dns-query, http-host
- domain: `storeedgefd.dsx.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `t-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `teams-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `update.googleapis.com`; roles: dns-query, tls-sni
- domain: `v10.events.data.microsoft.com`; roles: dns-query, tls-sni
- domain: `wpad.angrypoutine.com`; roles: dns-query
- domain: `www.bing.com`; roles: dns-query, tls-sni
- domain: `www.microsoft.com`; roles: dns-query, tls-sni
- domain: `www.msftncsi.com`; roles: dns-query, http-host
- ipv4: `0.0.0.0`; roles: network-endpoint
- ipv4: `10.9.10.102`; roles: dns-answer, network-endpoint

- ipv4: `10.9.10.103`; roles: dns-answer, network-endpoint
- ipv4: `10.9.10.255`; roles: network-endpoint
- ipv4: `10.9.10.9`; roles: dns-answer, network-endpoint
- ipv4: `104.125.253.131`; roles: dns-answer, network-endpoint
- ipv4: `104.215.148.63`; roles: dns-answer, network-endpoint
- ipv4: `104.46.162.226`; roles: dns-answer, network-endpoint
- ipv4: `13.107.136.254`; roles: dns-answer, network-endpoint
- ipv4: `13.107.18.254`; roles: dns-answer, network-endpoint
- ipv4: `13.107.21.200`; roles: dns-answer, network-endpoint
- ipv4: `13.107.246.254`; roles: dns-answer, network-endpoint
- ipv4: `13.107.3.254`; roles: dns-answer, network-endpoint
- ipv4: `13.107.49.254`; roles: dns-answer, network-endpoint
- ipv4: `13.107.5.88`; roles: dns-answer, network-endpoint
- ipv4: `13.69.239.72`; roles: dns-answer, network-endpoint
- ipv4: `13.77.161.179`; roles: dns-answer
- ipv4: `131.107.255.255`; roles: dns-answer
- ipv4: `167.172.37.9`; roles: network-endpoint
- ipv4: `169.254.181.227`; roles: network-endpoint
- ipv4: `169.254.255.255`; roles: network-endpoint
- ipv4: `172.217.168.195`; roles: dns-answer, network-endpoint
- ipv4: `184.85.229.68`; roles: dns-answer, network-endpoint
- ipv4: `194.62.42.206`; roles: dns-answer, network-endpoint
- ipv4: `20.140.48.71`; roles: dns-answer, network-endpoint
- ipv4: `20.189.173.7`; roles: dns-answer, network-endpoint
- ipv4: `20.190.151.131`; roles: dns-answer, network-endpoint
- ipv4: `20.190.151.132`; roles: dns-answer
- ipv4: `20.190.151.133`; roles: dns-answer
- ipv4: `20.190.151.134`; roles: dns-answer
- ipv4: `20.190.151.6`; roles: dns-answer
- ipv4: `20.190.151.68`; roles: dns-answer
- ipv4: `20.190.151.69`; roles: dns-answer
- ipv4: `20.190.151.9`; roles: dns-answer
- ipv4: `20.190.154.136`; roles: dns-answer
- ipv4: `20.190.154.138`; roles: dns-answer, network-endpoint
- ipv4: `20.190.154.139`; roles: dns-answer
- ipv4: `20.190.154.16`; roles: dns-answer
- ipv4: `20.190.154.17`; roles: dns-answer
- ipv4: `20.190.154.18`; roles: dns-answer
- ipv4: `20.190.154.19`; roles: dns-answer
- ipv4: `20.42.73.25`; roles: dns-answer, network-endpoint
- ipv4: `20.50.73.10`; roles: dns-answer, network-endpoint
- ipv4: `204.79.197.200`; roles: dns-answer, network-endpoint
- ipv4: `204.79.197.203`; roles: dns-answer, network-endpoint
- ipv4: `204.79.197.222`; roles: dns-answer, network-endpoint
- ipv4: `204.79.197.254`; roles: dns-answer, network-endpoint
- ipv4: `224.0.0.22`; roles: network-endpoint
- ipv4: `224.0.0.251`; roles: network-endpoint
- ipv4: `224.0.0.252`; roles: network-endpoint
- ipv4: `23.1.237.200`; roles: dns-answer, network-endpoint
- ipv4: `23.1.237.201`; roles: dns-answer, network-endpoint
- ipv4: `23.1.237.209`; roles: dns-answer
- ipv4: `23.1.237.216`; roles: dns-answer, network-endpoint
- ipv4: `23.1.237.225`; roles: dns-answer, network-endpoint
- ipv4: `23.100.36.182`; roles: dns-answer, network-endpoint
- ipv4: `23.3.6.28`; roles: dns-answer, network-endpoint
- ipv4: `23.3.84.67`; roles: dns-answer, network-endpoint
- ipv4: `23.3.85.202`; roles: dns-answer, network-endpoint
- ipv4: `23.3.85.234`; roles: dns-answer, network-endpoint
- ipv4: `23.3.86.10`; roles: dns-answer, network-endpoint
- ipv4: `239.255.255.250`; roles: http-host, network-endpoint
- ipv4: `255.255.255.255`; roles: network-endpoint
- ipv4: `34.117.59.81`; roles: dns-answer, network-endpoint
- ipv4: `40.112.72.205`; roles: dns-answer
- ipv4: `40.113.200.201`; roles: dns-answer
- ipv4: `40.125.122.151`; roles: dns-answer, network-endpoint

- ipv4: `40.126.26.132`; roles: dns-answer
- ipv4: `40.126.26.134`; roles: dns-answer
- ipv4: `40.126.26.135`; roles: dns-answer, network-endpoint
- ipv4: `40.76.4.15`; roles: dns-answer
- ipv4: `40.83.240.146`; roles: network-endpoint
- ipv4: `51.137.102.183`; roles: dns-answer, network-endpoint
- ipv4: `52.109.20.75`; roles: dns-answer
- ipv4: `52.109.76.32`; roles: dns-answer, network-endpoint
- ipv4: `52.109.76.36`; roles: network-endpoint
- ipv4: `52.109.8.19`; roles: network-endpoint
- ipv4: `52.109.8.22`; roles: dns-answer, network-endpoint
- ipv4: `52.109.8.25`; roles: dns-answer, network-endpoint
- ipv4: `52.113.196.254`; roles: dns-answer, network-endpoint
- ipv4: `52.137.106.217`; roles: dns-answer, network-endpoint
- ipv4: `52.182.143.208`; roles: dns-answer, network-endpoint
- ipv4: `52.184.217.20`; roles: dns-answer, network-endpoint
- ipv4: `52.238.248.6`; roles: dns-answer, network-endpoint
- ipv4: `52.242.101.226`; roles: dns-answer, network-endpoint
- ipv4: `52.242.97.97`; roles: dns-answer
- ipv4: `72.21.81.200`; roles: dns-answer, network-endpoint
- ipv4: `94.158.245.52`; roles: network-endpoint
- ipv4: `96.17.68.66`; roles: dns-answer, network-endpoint
- ipv4: `96.17.68.83`; roles: dns-answer
- ja3: `28a2c9bd18a11de089ef85a160da29e4`; roles: tls-client-fingerprint
- ja3: `37f463bf4616ecd445d4a1937da06e19`; roles: tls-client-fingerprint
- ja3: `3b5074b1b5d032e5620f69f9f700ff0e`; roles: tls-client-fingerprint
- ja3: `51c64c77e60f3980eeaa90869b68c58a8`; roles: tls-client-fingerprint
- ja3: `6271f898ce5be7dd52b0fc260d0662b3`; roles: tls-client-fingerprint
- ja3: `a0e9f5d64349fb13191bc781f81f42e1`; roles: tls-client-fingerprint
- sha256: `0076eaec4990322f0ebf53a5a53997c1525f358dc28dd6b7e1cbffd9bd41a9a5`; roles: exported-object
- sha256: `01b57c485bc90409c12dfff1fcc905e8ee03a18958ebb8fb7f007d317c2e6fc`; roles: exported-object
- sha256: `0550952e70d2e4e5ca28a8160e31cab6418ecb152915ec5dbfe88248d39fc2c7`; roles: exported-object
- sha256: `07a1470ae3b863578779e025fc6009e6519e0f77325e7a94a426a58b7e408196`; roles: exported-object
- sha256: `0c58b13a7b5d78c8a9e35d5995b7352c3b38acee77d6af9886c3cf2d668bfd3c`; roles: exported-object
- sha256: `0f132c40ca33c057af0aed28534cd23b31ce36da1ad0cda3f2c2f1e03d646bca`; roles: exported-object
- sha256: `0fb4d47bdcda9b77b0fbd8cb88b34ba180365991f6a376e00add1ac880b67fd8f`; roles: exported-object
- sha256: `1127774b7710ffa8c9bd5d3182517be848d9373e8f4382f28f801ba9e44f80fb`; roles: exported-object
- sha256: `153eec5b545f82f598d7728472073b1cddee325fc30cb7bc743c21d753610950d`; roles: exported-object
- sha256: `1d48d9166408d8b8bf39f9557e4f8a57133c353567c55966ec2831a7bc230431`; roles: exported-object
- sha256: `2972f477a28570de6c949fba237ace8c1bc2ea29b961b63aab3a57469e70cb51`; roles: exported-object
- sha256: `2ac413d79efa22e42a179f0450d7e8e4bb8202c881bf9e02a5a13a9a3626d792`; roles: exported-object
- sha256: `2cd96ea2a66b8bc4526b21c3744118b75f834d24739b04e2e7ceef21b8ad706f`; roles: exported-object
- sha256: `3197375f525ce4d0d339e56b343ecd510ffc72dcfa250b1352f8bd6a02d49864`; roles: exported-object
- sha256: `36d3e002691397fef5287603499d03fd0d929ebc2d4b08ece3d9e8b74cb3219`; roles: exported-object
- sha256: `4839da5b25468809fbc7708652e77c4aa945e6735bf5c9119b3299653898ce34`; roles: exported-object
- sha256: `4a11107d730c5943885081bfc3e902af14e8e83f59d110979bb2af47e325c38e`; roles: exported-object
- sha256: `4b03bfd94c00eecc15b41ef45adb7196c1bcfc942383b2ace3fac4a0423bdef4`; roles: exported-object
- sha256: `6137f8db2192e638e13610f75e73b9247c05f4706f0afd1fdb132d86de6b4012`; roles: exported-object
- sha256: `6a115a372e460c1de12760689955740a891b6d1e3f97bbe7e667c93ee940150c`; roles: exported-object
- sha256: `6c1eac65b98a81cd11abeaffe3fcf7f268e8788f733a0a8598b900201f05fc6d`; roles: exported-object
- sha256: `6db9e2137a8e70be66680ad4b9deeb177fc9f3103d9a1d9cde353f898de1bee`; roles: exported-object
- sha256: `729388a4d1b0e06eb28c982bf4a2e9304937ad1a92932dfc76d822b441563b6d`; roles: exported-object
- sha256: `809e5e4344a517b4f713aa55e03e2dc0c0d21cfa77ac2963e2e6e937e7d1264a`; roles: exported-object
- sha256: `80a71674cf8a71eaaf73c661d43ca1b69c4f393ccd603b89436812913ffbf0f1`; roles: exported-object
- sha256: `84520bc8bb4f129be41a7ab2a1ff1064efcd060d5521c2d5c23afd8710339411`; roles: exported-object
- sha256: `8529705a28a2cc8a6ac692e2f9a8cba5d6a3f44b81041270251389f1a017656c`; roles: exported-object
- sha256: `8eddb32e5ab1436d9cec5cbf730ad2a82d559730d69e35c534863d64d038d7c5`; roles: exported-object
- sha256: `9b8db510ef42b8ed54a3712636fda55a4f8cfd5493e20b74ab00cd4f3979f2d`; roles: exported-object
- sha256: `9db86bb697c7b6a5f3ed228546c9cb8a7037901e61efe0b244ba38e7d9ad3886`; roles: exported-object
- sha256: `b4effa72b591f85bed1dd07d82d924b9423f5e58a26c62290d11a628768676e4`; roles: exported-object
- sha256: `b80ed4f18c472ca7a6dd8dad53acc51a77e0ee0dc1fbadcc2e5d8e42efaa37fe`; roles: exported-object
- sha256: `b96661475f79113a3685ff208a52c3dde1340f93a479011f027c7bd3859c5334`; roles: exported-object
- sha256: `c1c72144b320890b971bf8cd335438dd6c2e50783398965e7891ccb30b4e3652`; roles: exported-object
- sha256: `cb82f8b3153b5c172ae382d0cf92ca5373017dd09f98137bc3b06982115006d7`; roles: exported-object
- sha256: `d98626686f7c56a852f3d658d947d96137ecbcedf278bdc2bc6158239a7434a2`; roles: exported-object

- sha256: `dd3eb184a16f533fccc480c533d93846a6bb11138dc12468830115263490238d`; roles: exported-object
- sha256: `e008608c81024ed297a07321b7c9ba9a00adac7cea71f24491af04b5e88f2f21`; roles: exported-object
- sha256: `e65eaf9faa6e7f3f0ce49c052a35be7cd5fed3ffc70b3f1ff7c213bee79f83fe`; roles: exported-object
- sha256: `e9132eaa61c1d06d76b82c27cfa7b6ba171f5e31fcec6fa78b03a7523f0f40a`; roles: exported-object
- sha256: `ea203eb1b56387cac02308b5aca040993e2d1c7fbd06413d41c957a726e4898f`; roles: exported-object
- sha256: `eddbff1244adffc83452a0a77a9c25fb8eb31625f9d18203acde9fd85eaa7f74`; roles: exported-object
- sha256: `eed363fc4af7a9070d69340592dcab7c78db4f90710357de29e3b624aa957cf8`; roles: exported-object
- sha256: `f040d968ae5f0c4324a4e3fce10f7bfb4370251aecb695f4a5f6c5af7a66aa7`; roles: exported-object
- sha256: `f7018b08490ebc04900ec28586710f3e93542ebe3ce390378e7f4e6665f28c43`; roles: exported-object
- url: `http://239.255.255.250:1900\*`; roles: http-request
- url: `http://au.download.windowsupdate.com/d/msdownload/update/software/defu/2021/09/am\_delta\_patch\_1.349.439.0\_dcf977cccce1b58289d270f71f8151b3acc1566b.exe`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8afe60e61b27f828`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?22c230ae05c29e0f`; roles: http-request
- url: `http://download.windowsupdate.com/c/msdownload/update/others/2021/09/35094710_046a1ec2fc584f3c2f6653542576b125ec45b91b.ca
b`; roles: http-request
- url: `http://download.windowsupdate.com/c/msdownload/update/others/2021/09/35094711_e3993b23840c0d600179f647e9ac08158269c095.c
ab`; roles: http-request
- url: `http://download.windowsupdate.com/c/msdownload/update/others/2021/09/35094827_769ef074432ee9d2982132709c97d7a039b1441d.c
ab`; roles: http-request
- url: `http://download.windowsupdate.com/c/msdownload/update/others/2021/09/35095041_d6f6e7dcab58bad491f97a8fb16f67acdd9c5880.ca
b`; roles: http-request
- url: `http://download.windowsupdate.com/c/msdownload/update/others/2021/09/35095042_571a24bf1c59b2fc66012aba76936bc63860b918.c
ab`; roles: http-request
- url: `http://download.windowsupdate.com/c/msdownload/update/others/2021/09/35095158_9a369166024cd2046a41b3fcf5a7d5743d20b1f8.ca
b`; roles: http-request
- url: `http://download.windowsupdate.com/c/msdownload/update/others/2021/09/35095401_461f0f3035a629e02f33b5439ab5d58c4e45c62f.ca
b`; roles: http-request
- url: `http://download.windowsupdate.com/c/msdownload/update/others/2021/09/35095402_3a3af9d09b295d5cad27c058b669144408fd1987.c
ab`; roles: http-request
- url: `http://download.windowsupdate.com/c/msdownload/update/others/2021/09/35095511_08bd8b8ea97b82600094601b9451b7fa9b028927.c
ab`; roles: http-request
- url: `http://download.windowsupdate.com/c/msdownload/update/others/2021/09/35097431_5695ed6029065d034bdbaa6edef143ec73f43570.c
ab`; roles: http-request
- url: `http://download.windowsupdate.com/c/msdownload/update/others/2021/09/35097432_b4cbace49a072b37958e15b9d3daadf28c89f361.c
ab`; roles: http-request
- url: `http://download.windowsupdate.com/c/msdownload/update/others/2021/09/35097541_59453a64ae1a0f59447d0c4e4bae68350827ad3f.c
ab`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35095718_d6052d2a18efec5d0584f7d9db0c6df36c871e5e.ca
b`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35095719_bb98167530418ae8aa387c077bca2d54e52a227b.
cab`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35095828_d42aac61fe6047b9b6b654db9d5c9ae957613125.c
ab`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35096071_6f89138c772d9cca2cda43656eecab96a5cd44fc.ca
b`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35096072_5331372f4a198d80f7a5602f73259ff77d004730.cab
`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35096188_49a74f42962e10ef9cfa9492f2c1955c24967958.ca
b`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35096401_980e49644362fb40897606d01fddd1ef79c6702a.ca
b`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35096402_83d0bc9d8970cab311753b171496293c4e0588b8.
cab`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35096518_246960552fd8974bcfe0af13e362f8d00f0c6046.cab
`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35096747_f2ef0a3546df9b0fe01091e8cf6244c2b18ad27a.cab
`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35096748_a533dd985a0175649c16855a9c628da8f21d78da.c
ab`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35096864_51f3f34383a28a4d5d63528d9978515e66a6806e.c
ab`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35097071_01580b64b700158e52507faa6223a4cb41c43f05.c
ab`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35097072_9c18abaa0dd4f3355c05cb1e0ac0d0a1da10552a.c

ab`; roles: http-request

- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35097188\_47bf5b9e41cf731eeaf7b93672b38948c413df0b.ca b`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35097759\_f51781226900f2c3a24cac0d25d7e32ce4232b12.c ab`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35097760\_94afc464b79c1922edc5d9f1aa46b8bbdafcac27.ca b`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35097869\_11f02196bd92ebd3ff0745749654d98eb8ddd58c.ca b`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35098112\_e6ce21ecdf7d899a6a8671574b68871ce853efe6.c ab`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35098113\_ea9c1c8bf8003ad3b08ee004e09ae3bbf5fb1456.ca b`; roles: http-request
- url: `http://download.windowsupdate.com/d/msdownload/update/others/2021/09/35098229\_d9a668acd9af16621c688b823ada2c10de963ca4.c ab`; roles: http-request
- url: `http://simpsonsavings.com/bmdff/BhoHsCtZ/MLdmpfjX/5uFG3Dz7yt/date1?BNLV65=pAAS`; roles: http-request
- url: `http://store-images.s-microsoft.com/image/apps.11608.14255546098955437.c2922c50-eb00-4f80-b393-4e513d9f81c7.4345eb8f-f893-40 a2-aec5-20f4758af165?w=150&h=150`; roles: http-request
- url: `http://store-images.s-microsoft.com/image/apps.16525.14618985536919905.4b30e4f3-f7a1-4421-840c-2cc97b10e8e0.13409c3f-0e0f-40 dd-b458-b324f658c185?w=150&h=150`; roles: http-request
- url: `http://store-images.s-microsoft.com/image/apps.16999.13510798885065391.a43a9782-6060-4560-b391-7f6f188559d0.dc15b6ee-644d-4 1e3-8d76-67c8c9dac9e9?w=150&h=225`; roles: http-request
- url: `http://store-images.s-microsoft.com/image/apps.28261.13798539581762600.abe1643f-1704-4a4d-a61b-47ccc25da012.ada314ec-db8e-4 9bb-a756-60487526418e?w=150&h=150`; roles: http-request
- url: `http://store-images.s-microsoft.com/image/apps.31617.13655054093851568.f2bf9430-60d7-4569-a50d-0f21c9ade6b3.c563d383-997d-4d a1-9def-d7200e3547f8?w=150&h=150`; roles: http-request
- url: `http://store-images.s-microsoft.com/image/apps.40518.14127333176902609.7be7b901-15fe-4c27-863c-7c0dbfc26c5c.5c278f58-912b-4af 9-88f8-a65fff2da477?w=150&h=150`; roles: http-request
- url: `http://www.msftncsi.com/ncsi.txt`; roles: http-request
- user_agent: `Microsoft NCSI`; roles: http-client
- user_agent: `Microsoft-CryptoAPI/10.0`; roles: http-client
- user_agent: `Microsoft-Delivery-Optimization/10.0`; roles: http-client
- user_agent: `Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CL R 3.0.30729; .NET CLR 3.5.30729)`; roles: http-client
- user_agent: `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edg e/18.19043`; roles: http-client
- user_agent: `Windows-Update-Agent/10.0.10011.16384 Client-Protocol/2.32`; roles: http-client
- exported object `am\_delta\_patch\_1.349.439.0\_dcf977cccce1b58289d270f71f8151b3acc1566b(3).exe`; SHA-256 `1d48d9166408d8b8bf39f95 57e4f8a57133c353567c55966ec2831a7bc230431`; size 1048576 bytes
Static content: `{"content\_kind":"pe","features":[],"inspected\_bytes":262144,"inspection\_truncated":true,"interpretation":"Static content only; not proof of execution, intent, or malware family"}`. Not execution proof.
- exported object `am\_delta\_patch\_1.349.439.0\_dcf977cccce1b58289d270f71f8151b3acc1566b(2).exe`; SHA-256 `2ac413d79efa22e42a179f0 450d7e8e4bb8202c881bf9e02a5a13a9a3626d792`; size 1048576 bytes
Static content: `{"content\_kind":"script-like-text","features":{"excerpt":"IEx","feature":{"dynamic-evaluation","offset":207057}},"inspected\_bytes":2 62144,"inspection\_truncated":true,"interpretation":"Static content only; not proof of execution, intent, or malware family"}`. Not execution proof.
- exported object `date1%3fBNLV65=pAAS`; SHA-256 `eed363fc4af7a9070d69340592dcab7c78db4f90710357de29e3b624aa957cf8`; size 284 816 bytes
Static content: `{"content\_kind":"pe","features":[],"inspected\_bytes":262144,"inspection\_truncated":true,"interpretation":"Static content only; not proof of execution, intent, or malware family"}`. Not execution proof.
- exported object `am\_delta\_patch\_1.349.439.0\_dcf977cccce1b58289d270f71f8151b3acc1566b(4).exe`; SHA-256 `0fb4d47bcd49b77b0fbd8cb 88b34ba180365991f6a376e00add1ac880b67fd8f`; size 922056 bytes
- exported object `apps.40518.14127333176902609.7be7b901-15fe-4c27-863c-7c0dbfc26c5c.5c278f58-912b-4af9-88f8-a65fff2da477%3fw=15 0&h=150`; SHA-256 `c1c72144b320890b971bf8cd335438dd6c2e50783398965e7891ccb30b4e3652`; size 24101 bytes
- exported object `apps.16525.14618985536919905.4b30e4f3-f7a1-4421-840c-2cc97b10e8e0.13409c3f-0e0f-40dd-b458-b324f658c185%3fw=1 50&h=150`; SHA-256 `f7018b08490ebc04900ec28586710f3e93542ebe3ce390378e7f4e6665f28c43`; size 19230 bytes
- exported object `apps.31617.13655054093851568.f2bf9430-60d7-4569-a50d-0f21c9ade6b3.c563d383-997d-4da1-9def-d7200e3547f8%3fw= 150&h=150`; SHA-256 `0c58b13a7b5d78c8a9e35d5995b7352c3b38acee77d6af9886c3cf2d668bfd3c`; size 17906 bytes
- exported object `apps.16999.13510798885065391.a43a9782-6060-4560-b391-7f6f188559d0.dc15b6ee-644d-41e3-8d76-67c8c9dac9e9%3fw =150&h=225`; SHA-256 `4a1107d730c5943885081bfc3e902af14e8e83f59d110979bb2af47e325c38e`; size 16870 bytes
- exported object `apps.11608.14255546098955437.c2922c50-eb00-4f80-b393-4e513d9f81c7.4345eb8f-f893-40a2-aec5-20f4758af165%3fw=1 50&h=150`; SHA-256 `0f132c40ca33c057af0aed28534cd23b31ce36da1ad0cda3f2c2f1e03d646bca`; size 13972 bytes
- exported object `35098229\_d9a668acd9af16621c688b823ada2c10de963ca4.cab`; SHA-256 `4b03bfd94c00eccc15b41ef45adb7196c1bcfc94 2383b2ace3fac4a0423bdef4`; size 10821 bytes
- exported object `35094827\_769ef074432ee9d2982132709c97d7a039b1441d.cab`; SHA-256 `4839da5b25468809fbc7708652e77c4aa945e67 35bf5c9119b3299653898ce34`; size 10791 bytes

- exported object `35096864\_51f3f34383a28a4d5d63528d9978515e66a6806e.cab`; SHA-256 `cb82f8b3153b5c172ae382d0cf92ca5373017dd09f98137bc3b06982115006d7`; size 10789 bytes

- exported object `35096188\_49a74f42962e10ef9cfa9492f2c1955c24967958.cab`; SHA-256 `2972f477a28570de6c949fba237ace8c1bc2ea29b961b63aab3a57469e70cb51`; size 10781 bytes

- exported object `35096518\_246960552fd8974bcfe0af13e362f8d00f0c6046.cab`; SHA-256 `8529705a28a2cc8a6ac692e2f9a8cba5d6a3f44b81041270251389f1a017656c`; size 10767 bytes

- exported object `35095158\_9a369166024cd2046a41b3fcf5a7d5743d20b1f8.cab`; SHA-256 `1127774b7710ffa8c9bd5d3182517be848d9373e8f4382f28f801ba9e44f80fb`; size 10765 bytes

- exported object `35097188\_47bf5b9e41cf731eeaf7b93672b38948c413df0b.cab`; SHA-256 `80a71674cf8a71eaa7f3c661d43ca1b69c4f393ccd603b89436812913fffb0f1`; size 10763 bytes

- exported object `35095511\_08bd8b8ea97b82600094601b9451b7fa9b028927.cab`; SHA-256 `07a1470ae3b863578779e025fc6009e6519e0f77325e7a94a426a58b7e408196`; size 10623 bytes

- exported object `35097541\_59453a64ae1a0f59447d0c4e4bae68350827ad3f.cab`; SHA-256 `e9132eaa61c1d06d76b82c27cfa7b6ba171f5e31fcec6fa78b03a7523f0f40a`; size 10621 bytes

- exported object `35095828\_d42aac61fe6047b9b6b654db9d5c9ae957613125.cab`; SHA-256 `dd3eb184a16f533fce480c533d93846a6bb11138dc12468830115263490238d`; size 10593 bytes

- exported object `35097869\_11f02196bd92ebd3ff0745749654d98eb8ddd58c.cab`; SHA-256 `0076eae4990322f0ebf53a5a53997c1525f358dc28dd6b7e1cbffd9bd41a9a5`; size 10589 bytes

- exported object `35096748\_a533dd985a0175649c16855a9c628da8f21d78da.cab`; SHA-256 `9db86bb697c7b6a5f3ed228546c9cb8a7037901e61efe0b244ba38e7d9ad3886`; size 7287 bytes

- exported object `35098113\_ea9c1c8bf8003ad3b08ee004e09ae3bbf5fb1456.cab`; SHA-256 `01b57c485bc90409c12dfff1fcca905e8ee03a18958ebb8fb7f007d317c2e6fc`; size 7285 bytes

- exported object `35096747\_f2ef0a3546df9b0fe01091e8cf6244c2b18ad27a.cab`; SHA-256 `2cd96ea2a66b8bc4526b21c3744118b75f834d24739b04e2e7ceef21b8ad706f`; size 7285 bytes

- exported object `35096072\_5331372f4a198d80f7a5602f73259ff77d004730.cab`; SHA-256 `6db9e2137a8e7ebe66680ad4b9deeb17f7fc9f3103d9a1d9cde353f898de1bee`; size 7283 bytes

- exported object `35098112\_e6ce21ecd7d899a6a8671574b68871ce853efe6.cab`; SHA-256 `d98626686f7c56a852f3d658d947d96137ecbcfe d278bdc2bc6158239a7434a2`; size 7277 bytes

- exported object `35094710\_046a1ec2fc584f3c2f6653542576b125ec45b91b.cab`; SHA-256 `ea203eb1b56387cac02308b5aca040993e2d1c7fbd06413d41c957a726e4898f`; size 7277 bytes

- exported object `35096071\_6f89138c772d9cca2cda43656eeca96a5cd44fc.cab`; SHA-256 `153eec5b545f82f598d7728472073b1cdee325fc30cb7bc743c21d753610950d`; size 7275 bytes

- exported object `35097432\_b4cbace49a072b37958e15b9d3daadf28c89f361.cab`; SHA-256 `729388a4d1b0e06eb28c982bf4a2e9304937ad1a92932dfc76d822b441563b6d`; size 7275 bytes

- exported object `35094711\_e3993b23840c0d600179f647e9ac08158269c095.cab`; SHA-256 `e008608c81024ed297a07321b7c9ba9a00adac7cea71f24491af04b5e88f2f21`; size 7275 bytes

- exported object `35097431\_5695ed6029065d034bdbaa6edef143ec73f43570.cab`; SHA-256 `8eddb32e5ab1436d9cec5cbf730ad2a82d559730d69e35c534863d64d038d7c5`; size 7273 bytes

- exported object `35095402\_3a3af9d09b295d5cad27c058b669144408fd1987.cab`; SHA-256 `3197375f525ce4d0d339e56b343ecd510ffc72dcfa250b1352f8bd6a02d49864`; size 7267 bytes

- exported object `35095401\_461f0f3035a629e02f33b5439ab5d58c4e45c62f.cab`; SHA-256 `f040d968ae5f0c4324a4e3fce10f7bfbc4370251aeb695f4a5f6c5af7a66aa7`; size 7261 bytes

- exported object `35097072\_9c18abaa0dd4f3355c05cb1e0ac0d0a1da10552a.cab`; SHA-256 `6c1eac65b98a81cd11abeaffe3fcf7f268e8788f733a0a8598b900201f05fc6d`; size 7189 bytes

- exported object `35097071\_01580b64b700158e52507faa6223a4cb41c43f05.cab`; SHA-256 `0550952e70d2e4e5ca28a8160e31cab6418ecb152915ec5dbfe88248d39fc2c7`; size 7185 bytes

- exported object `35096401\_980e49644362fb40897606d01fddd1ef79c6702a.cab`; SHA-256 `b4effa72b591f85bed1dd07d82d924b9423f5e58a26c62290d11a628768676e4`; size 7183 bytes

- exported object `35096402\_83d0bc9d8970cab311753b171496293c4e0588b8.cab`; SHA-256 `36d3e002691397fed5287603499d03fd0d929ebc2d4b08ece3d9e8b74cb3219`; size 7181 bytes

- exported object `35095042\_571a24bf1c59b2fc66012aba76936bc63860b918.cab`; SHA-256 `e65eaf9faa6e7f3f0ce49c052a35be7cd5fed3ffc70b3f1ff7c213bee79f83fe`; size 7181 bytes

- exported object `35097759\_f51781226900f2c3a24cac0d25d7e32ce4232b12.cab`; SHA-256 `809e5e4344a517b4f713aa55e03e2dc0c0d21cfa77ac2963e2e6e937e7d1264a`; size 7175 bytes

- exported object `35097760\_94afc464b79c1922edc5d9f1aa46b8bbdafcac27.cab`; SHA-256 `b96661475f79113a3685ff208a52c3dde1340f93a479011f027c7bd3859c5334`; size 7175 bytes

- exported object `35095719\_bb98167530418ae8aa387c077bca2d54e52a227b.cab`; SHA-256 `6a115a372e460c1de12760689955740a891b6d1e3f97bbe7e667c93ee940150c`; size 7171 bytes

- exported object `35095718\_d6052d2a18efec5d0584f7d9db0c6df36c871e5e.cab`; SHA-256 `b80ed4f18c472ca7a6dd8dad53acc51a77e0ee0dc1fbadcc2e5d8e42efaa37fe`; size 7171 bytes

- exported object `35095041\_d6fbe7dcab58bad491f97a8fb16f67acdd9c5880.cab`; SHA-256 `eddbff1244adffc83452a0a77a9c25fb8eb31625f9d18203acde9fd85eaa7f74`; size 7171 bytes

- exported object `apps.28261.13798539581762600.abe1643f-1704-4a4d-a61b-47ccc25da012.ada314ec-db8e-49bb-a756-60487526418e%3fw=150&h=150`; SHA-256 `84520bc8bb4f129be41a7ab2a1ff1064efcd060d5521c2d5c23afd8710339411`; size 2222 bytes

- exported object `ncsi.txt`; SHA-256 `6137f8db2192e638e13610f75e73b9247c05f4706f0afd1fdb132d86de6b4012`; size 14 bytes

- exported object `am\_delta\_patch\_1.349.439.0\_dcf977cccce1b58289d270f71f8151b3acc1566b(1).exe`; SHA-256 `9b8db510ef42b8ed54a3712636fda55a4f8cfd5493e20b74ab00cd4f3979f2d`; size 2 bytes

Actor similarity leads

- Volatile Cedar (G0123): 20% TTP overlap. This is an investigation lead, not attribution.
- Winnti Group (G0044): 17% TTP overlap. This is an investigation lead, not attribution.
- Ajax Security Team (G0130): 17% TTP overlap. This is an investigation lead, not attribution.
- IndigoZebra (G0136): 14% TTP overlap. This is an investigation lead, not attribution.
- Nomadic Octopus (G0133): 14% TTP overlap. This is an investigation lead, not attribution.
- Whitefly (G0107): 11% TTP overlap. This is an investigation lead, not attribution.
- Metador (G1013): 11% TTP overlap. This is an investigation lead, not attribution.
- Elderwood (G0066): 11% TTP overlap. This is an investigation lead, not attribution.
- Rancor (G0075): 11% TTP overlap. This is an investigation lead, not attribution.
- Evilnum (G0120): 9% TTP overlap. This is an investigation lead, not attribution.

Local enrichment and correlations

No match means unknown in this corpus. Local CTI may postdate the capture. Matches and shared infrastructure require review; no automatic promotion or attribution.

Snapshot: `fd1ef8f35792013eb051dd90b6a512f313f5655d99849d97a044c7dc6beb785f`; recorded 2026-09-19T12:10:32.214995+00:00; mode: local-only.

Coverage: `{ "matched\_observables":0, "no\_exact\_match":248, "observable\_limit":5000, "observables\_checked":248, "observables\_total":248, "prior\_case\_limit\_reached":false, "prior\_cases\_checked":15, "truncated":false }`

- Catalog T1105: <https://attack.mitre.org/techniques/T1105>; detection strategies: `{ "attack\_id":"DET0060", "name":"Detect Ingress Tool Transfers via Behavioral Chain", "stix\_id":"x-mitre-detection-strategy--67677c4c-5778-49eb-ae74-1920645b8554" }`
- Prior analysis `8f0da1cd-9998-4d41-9fc7-683302a6ee24` shares 51 observations. This does not establish a common campaign.
- Prior analysis `96e0e828-93ae-49d5-8104-9f14cb584c3e` shares 23 observations. This does not establish a common campaign.
- Prior analysis `6e50c68f-5552-400c-9835-15867ddb022d` shares 23 observations. This does not establish a common campaign.
- Prior analysis `43bc93eb-d6db-4400-b983-b0dd404c8ca4` shares 35 observations. This does not establish a common campaign.
- Prior analysis `6df36b51-4b44-4660-b534-2fa89705e807` shares 35 observations. This does not establish a common campaign.
- Prior analysis `29aa3ef8-47c9-4c47-b4cc-1ff3e0708142` shares 10 observations. This does not establish a common campaign.
- Prior analysis `b79032a8-d69e-4ac1-bdd4-542473fa8e3b` shares 15 observations. This does not establish a common campaign.
- Prior analysis `faf041c3-70e0-4a01-8780-10917e5e187c` shares 12 observations. This does not establish a common campaign.
- Prior analysis `08324647-35af-4af2-8d82-4387eec03918` shares 14 observations. This does not establish a common campaign.
- Prior analysis `616a90fa-f15e-4fcb-8d56-7b8e0eff5785` shares 4 observations. This does not establish a common campaign.
- Prior analysis `459e119d-191f-49e8-85ea-c78f9de41826` shares 15 observations. This does not establish a common campaign.
- Prior analysis `7a2cfe72-f48d-4894-8a2d-8889cb3b11b2` shares 12 observations. This does not establish a common campaign.
- Prior analysis `81373b30-6a59-49d1-89b0-bad73ed19eaa` shares 13 observations. This does not establish a common campaign.
- Prior analysis `38851ad7-b3a0-423d-ae89-3b7be4e4b908` shares 21 observations. This does not establish a common campaign.
- Prior analysis `bfccc426-aa9b-4007-8558-a66d37ecb90c` shares 18 observations. This does not establish a common campaign.
- External provider queries: 0. Not requested; no unknown indicator is classified as benign.

Coverage and limitations

- Packet and protocol facts are deterministic for the recorded analyzer manifest.
- Encrypted application payloads are not decrypted; only available metadata is reported.
- ATT&CK mappings and actor overlaps are candidates until analyst review and promotion.
- HTTP object inventory: `{ "compact_objects":0, "complete":true, "detailed_objects":45, "exported_objects":46, "hashed_bytes":3675348, "hashed_objects":46, "omitted_unique_hashes":0, "returned_unique_hashes":45, "selection":"content-classified first, then size descending, SHA256 tie-break; deduplicated by full hash; overflow retains a compact hash index", "unhashed_objects":0, "unique_hashes":45 }`. Compact overflow hashes are retained in JSON coverage and observables.
- A directory subject is not necessarily a logged-in user; consult identity bindings in the JSON evidence.
- Rendered / available: findings 9/9, identities 4/4, observables 248/248, artifacts 45/45. Full returned inventory is in the JSON result.