

AdversaryGraph

Threat Intelligence Analysis Report

Analysis Metadata

Provider:	deterministic
Model:	tshark-evidence-v3
Domain:	enterprise-attack
Session ID:	a894fbbc-d0d5-4309-bd04-2eda8773adfa
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 18189 packets across 75 IP endpoints and 698 transport flows. Observed 430 DNS events, 404 HTTP requests, 174 TLS ClientHello events, and 18 exported HTTP object(s). Deterministic rules produced 8 finding(s): 1 high, 0 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: 32231 / 32231 characters
Promotion ready: No

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

Promotion blockers

- 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: 2024-08-15-traffic-analysis-exercise.pcap

Capture SHA-256: `e154de6895c5f0a9edd07b1279b33014507236dbb44a449790c255b87a327a3c`

Semantic result SHA-256: `f1e40c750b6946d0db5734f3fb390579d65b42e1dbb9cdd67b0a5c6d2f3174ab`

Analyzer manifest SHA-256: `ee952aeb7cdc6958f4ae5178c54c274a1e4f0aec4d42f3bdb95baaff063b3dde`

Executive summary

Decoded 18189 packets across 75 IP endpoints and 698 transport flows. Observed 430 DNS events, 404 HTTP requests, 174 TLS ClientHello events, and 18 exported HTTP object(s). Deterministic rules produced 8 finding(s): 1 high, 0 medium, and 7 low. Findings are evidence-bound candidates and require analyst review; encrypted payload contents remain unavailable.

Capture facts

- Packets: 18189
- Duration: 1962.204948 seconds
- Captured bytes: 11674125
- Endpoints: 75
- Flows: 698

Deterministic findings

HIGH \u2014 Periodic HTTP callback pattern

Repeated requests have a stable cadence consistent with automated callback or beacon behavior.

Rule: `periodic-http-callbacks@pcap-rules-v3`; confidence: 0.88; evidence: frame 11028 / TCP stream 142, frame 11505 / TCP stream 145, frame 11619 / TCP stream 151, frame 11688 / TCP stream 155, frame 11962 / TCP stream 164.

Metrics: `{ "destination": "72.5.43.29", "host": "72.5.43.29", "median\_absolute\_deviation": 1.037, "median\_interval\_seconds": 5.685, "method": "GET", "port": 80, "request\_count": 303, "source": "10.8.15.133", "uri": "/" }`

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 56, frame 60, frame 962, frame 964, frame 2106.

Metrics: `{ "domain": "wpad.lafontainebleu.org", "response\_count": 20, "source": "10.8.15.133" }`

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 281 / TCP stream 11, frame 285 / TCP stream 11, frame 292 / TCP stream 11, frame 297 / TCP stream 11, frame 312 / TCP stream 11.

Metrics: `{ "destination": "10.8.15.4", "event\_count": 69, "operation\_numbers": [ "0", "1", "12", "13", "30" ], "protocol": "drsuapi", "source": "10.8.15.133" }`

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 37 / TCP stream 0, frame 288 / TCP stream 19, frame 295 / TCP stream 19, frame 300 / TCP stream 19, frame 304 / TCP stream 19.

Metrics: `{"destination":"10.8.15.4","event\_count":143,"operation\_numbers":["","0","2","3"],"protocol":"ldap","source":"10.8.15.133"}`

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 1096 / TCP stream 1, frame 1098 / TCP stream 1, frame 1100 / TCP stream 1, frame 1102 / TCP stream 1, frame 1104 / TCP stream 1.

Metrics: `{"destination":"10.8.15.4","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"10.8.15.133"}`

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 282 / TCP stream 11, frame 287 / TCP stream 11, frame 293 / TCP stream 11, frame 298 / TCP stream 11, frame 313 / TCP stream 11.

Metrics: `{"destination":"10.8.15.133","event\_count":69,"operation\_numbers":["0","1","12","13","30"],"protocol":"drsuapi","source":"10.8.15.4"}`

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 39 / TCP stream 0, frame 290 / TCP stream 19, frame 299 / TCP stream 19, frame 302 / TCP stream 19, frame 305 / TCP stream 19.

Metrics: `{"destination":"10.8.15.133","event\_count":113,"operation\_numbers":["","1","4,19,19,19,5","4,5","5"],"protocol":"ldap","source":"10.8.15.4"}`

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 1097 / TCP stream 1, frame 1099 / TCP stream 1, frame 1101 / TCP stream 1, frame 1103 / TCP stream 1, frame 1105 / TCP stream 1.

Metrics: `{"destination":"10.8.15.133","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"10.8.15.4"}`

ATT&CK candidates

- T1071.001 Application Layer Protocol: Web Protocols (command-and-control), confidence=0.85, status=suggested; basis=versioned-deterministic-rule.

Identities

- account: `desktop-h8alzvbv\$`; client IPs: 10.8.15.133; frames: 151, 166, 169, 173, 187
- account: `plucero`; client IPs: 10.8.15.133; frames: 975, 983, 985, 997, 1011
- full-name: `Pierce Lucero`; client IPs: 10.8.15.133; frames: 1111
- hostname: `DESKTOP-H8ALZBV`; client IPs: 10.8.15.133; frames: 1, 3, 5, 30, 58
- netbios-group: `LAFONTAINEBLEU`; client IPs: unbound subject; frames: 31, 57, 103, 447

IOC and artifact candidates

- domain: `a1834.dscg2.akamai.net`; roles: dns-cname
- domain: `acroipm2.adobe.com`; roles: dns-query, http-host
- domain: `api.msn.com`; roles: dns-query, tls-sni
- domain: `app-edge.smartscreen.microsoft.com`; roles: dns-query, tls-sni

- domain: `armmf.adobe.com`; roles: dns-query, tls-sni
- domain: `assets.msn.com`; roles: dns-query, tls-sni
- domain: `blob.mwh03prd02a.store.core.windows.net`; roles: dns-cname
- domain: `browser.events.data.msn.com`; roles: dns-query, tls-sni
- domain: `business.bing.com`; roles: dns-query, tls-sni
- domain: `business.checkfedexp.com`; roles: dns-query, tls-sni
- domain: `bzib.nelreports.net`; roles: dns-query, tls-sni
- domain: `c-msn-com-nsatc.trafficmanager.net`; roles: dns-cname
- domain: `c-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `c.bing.com`; roles: dns-query, tls-sni
- domain: `c.msn.com`; roles: dns-query, tls-sni
- domain: `client.wns.windows.com`; roles: dns-query, tls-sni
- domain: `cxcs.microsoft.net`; roles: dns-query, tls-sni
- domain: `default.exp-tas.com`; roles: dns-query, tls-sni
- domain: `displaycatalog.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `dl-edge.smartscreen.microsoft.com`; roles: dns-query
- domain: `dual-s-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `ecn-us.dev.virtualearth.net`; roles: dns-query, tls-sni
- domain: `ecs.office.com`; roles: dns-query, tls-sni
- domain: `edge-consumer-static.azureedge.net`; roles: dns-query, tls-sni
- domain: `edge-microsoft-com.dual-a-0036.a-msedge.net`; roles: dns-cname
- domain: `edge.microsoft.com`; roles: dns-query, tls-sni
- domain: `edgeservices.bing.com`; roles: dns-query, tls-sni
- domain: `fd.api.iris.microsoft.com`; roles: dns-query, tls-sni
- domain: `fe2cr.update.microsoft.com`; roles: dns-query, tls-sni
- domain: `fe2cr.update.msft.com.trafficmanager.net`; roles: dns-cname
- domain: `fe3cr.delivery.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `fp.msedge.net`; roles: dns-query, tls-sni
- domain: `g.live.com`; roles: dns-query, tls-sni
- domain: `go.microsoft.com`; roles: dns-query, tls-sni
- domain: `img-s-msn-com.akamaized.net`; roles: dns-query, tls-sni
- domain: `img.s-msn.com`; roles: dns-query, tls-sni
- domain: `licensing.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `login.microsoftonline.com`; roles: dns-query, tls-sni
- domain: `mobile.events.data.microsoft.com`; roles: dns-query, tls-sni
- domain: `mrodevicemgr.officeapps.live.com`; roles: dns-query, tls-sni
- domain: `msedge.b.tlu.dl.delivery.mp.microsoft.com`; roles: dns-query, http-host
- domain: `nav-edge.smartscreen.microsoft.com`; roles: dns-query, tls-sni
- domain: `nav.smartscreen.microsoft.com`; roles: dns-query, tls-sni
- domain: `ntp.msn.com`; roles: dns-query, tls-sni
- domain: `odc.officeapps.live.com`; roles: dns-query, tls-sni
- domain: `officeclient.microsoft.com`; roles: dns-query, tls-sni
- domain: `oneclient.sfx.ms`; roles: dns-query, tls-sni
- domain: `oneocsp.microsoft.com`; roles: dns-query, http-host
- domain: `ow1.res.office365.com`; roles: dns-query, tls-sni
- domain: `prod.mrodevicemgr.live.com.akadns.net`; roles: dns-cname
- domain: `pti.store.microsoft.com`; roles: dns-query
- domain: `quote.checkfedexp.com`; roles: dns-query, http-host
- domain: `r-msftstatic-com.a-0016.a-msedge.net`; roles: dns-cname
- domain: `r.bing.com`; roles: dns-query, tls-sni
- domain: `r.msftstatic.com`; roles: dns-query, tls-sni
- domain: `sb.scorecardresearch.com`; roles: dns-query, tls-sni
- domain: `settings-win.data.microsoft.com`; roles: dns-query, tls-sni
- domain: `srtb.msn.com`; roles: dns-query, tls-sni
- domain: `storecatalogrevocation.storequality.microsoft.com`; roles: dns-query, tls-sni
- domain: `th.bing.com`; roles: dns-query, tls-sni
- domain: `v10.events.data.microsoft.com`; roles: dns-query, tls-sni
- domain: `v20.events.data.microsoft.com`; roles: dns-query, tls-sni
- domain: `weathermapdata.blob.core.windows.net`; roles: dns-query, tls-sni
- domain: `win-jegjix7q9rs.lafontainebleu.org`; roles: dns-query
- domain: `windows.msn.com`; roles: dns-query, tls-sni
- domain: `wns.notify.trafficmanager.net`; roles: dns-cname
- domain: `wpad.lafontainebleu.org`; roles: dns-query
- domain: `www.bing.com`; roles: dns-query, tls-sni
- domain: `www.msftconnecttest.com`; roles: dns-query, http-host

- domain: `www.msn.com`; roles: dns-query, tls-sni
- ipv4: `0.0.0.0`; roles: network-endpoint
- ipv4: `10.8.15.133`; roles: network-endpoint
- ipv4: `10.8.15.255`; roles: network-endpoint
- ipv4: `10.8.15.4`; roles: dns-answer, network-endpoint
- ipv4: `104.21.55.70`; roles: dns-answer, network-endpoint
- ipv4: `104.40.82.182`; roles: dns-answer, network-endpoint
- ipv4: `13.107.21.237`; roles: dns-answer, network-endpoint
- ipv4: `13.107.21.239`; roles: dns-answer, network-endpoint
- ipv4: `13.107.246.57`; roles: dns-answer, network-endpoint
- ipv4: `13.107.4.254`; roles: dns-answer, network-endpoint
- ipv4: `13.107.5.93`; roles: dns-answer, network-endpoint
- ipv4: `13.107.6.158`; roles: dns-answer, network-endpoint
- ipv4: `13.70.79.200`; roles: dns-answer, network-endpoint
- ipv4: `13.85.23.206`; roles: dns-answer, network-endpoint
- ipv4: `13.89.179.13`; roles: dns-answer, network-endpoint
- ipv4: `172.67.170.159`; roles: dns-answer, network-endpoint
- ipv4: `18.160.156.115`; roles: dns-answer, network-endpoint
- ipv4: `18.160.156.14`; roles: dns-answer
- ipv4: `18.160.156.41`; roles: dns-answer
- ipv4: `18.160.156.89`; roles: dns-answer
- ipv4: `199.232.210.172`; roles: dns-answer, network-endpoint
- ipv4: `199.232.214.172`; roles: dns-answer
- ipv4: `20.10.31.115`; roles: dns-answer, network-endpoint
- ipv4: `20.125.209.212`; roles: dns-answer, network-endpoint
- ipv4: `20.163.45.186`; roles: dns-answer
- ipv4: `20.189.173.9`; roles: dns-answer, network-endpoint
- ipv4: `20.190.157.9`; roles: dns-answer
- ipv4: `20.241.44.114`; roles: dns-answer, network-endpoint
- ipv4: `20.25.227.174`; roles: dns-answer, network-endpoint
- ipv4: `20.3.0.251`; roles: dns-answer, network-endpoint
- ipv4: `20.42.65.88`; roles: dns-answer, network-endpoint
- ipv4: `20.42.65.94`; roles: dns-answer, network-endpoint
- ipv4: `20.42.72.131`; roles: dns-answer, network-endpoint
- ipv4: `20.44.10.122`; roles: dns-answer, network-endpoint
- ipv4: `20.60.228.1`; roles: dns-answer, network-endpoint
- ipv4: `20.96.153.111`; roles: dns-answer, network-endpoint
- ipv4: `20.99.184.37`; roles: dns-answer, network-endpoint
- ipv4: `204.79.197.203`; roles: dns-answer, network-endpoint
- ipv4: `204.79.197.219`; roles: dns-answer, network-endpoint
- ipv4: `204.79.197.222`; roles: dns-answer, network-endpoint
- ipv4: `204.79.197.237`; roles: dns-answer
- ipv4: `204.79.197.239`; 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: `23.194.68.140`; roles: dns-answer, network-endpoint
- ipv4: `23.195.200.230`; roles: dns-answer, network-endpoint
- ipv4: `23.205.110.12`; roles: dns-answer, network-endpoint
- ipv4: `23.205.110.48`; roles: dns-answer, network-endpoint
- ipv4: `23.205.110.59`; roles: dns-answer
- ipv4: `23.205.110.62`; roles: dns-answer
- ipv4: `23.215.55.139`; roles: dns-answer, network-endpoint
- ipv4: `23.215.55.144`; roles: dns-answer
- ipv4: `23.220.103.18`; roles: dns-answer, network-endpoint
- ipv4: `23.220.103.72`; roles: dns-answer, network-endpoint
- ipv4: `23.220.103.78`; roles: dns-answer
- ipv4: `23.220.103.8`; roles: dns-answer, network-endpoint
- ipv4: `23.220.251.196`; roles: dns-answer
- ipv4: `23.220.251.208`; roles: dns-answer, network-endpoint
- ipv4: `23.221.36.164`; roles: dns-answer, network-endpoint
- ipv4: `23.223.31.29`; roles: dns-answer
- ipv4: `23.223.31.31`; roles: dns-answer
- ipv4: `23.223.31.32`; roles: dns-answer
- ipv4: `23.223.31.33`; roles: dns-answer

- ipv4: `23.223.31.34`; roles: dns-answer, network-endpoint
- ipv4: `23.223.31.36`; roles: dns-answer
- ipv4: `23.223.31.37`; roles: dns-answer
- ipv4: `23.223.31.39`; roles: dns-answer
- ipv4: `23.223.31.40`; roles: dns-answer
- ipv4: `23.33.138.184`; roles: dns-answer, network-endpoint
- ipv4: `23.43.244.167`; roles: dns-answer, network-endpoint
- ipv4: `23.53.13.196`; roles: dns-answer, network-endpoint
- ipv4: `23.53.13.197`; roles: dns-answer, network-endpoint
- ipv4: `23.53.13.198`; roles: dns-answer
- ipv4: `23.53.13.199`; roles: dns-answer
- ipv4: `23.53.13.200`; roles: dns-answer
- ipv4: `23.53.13.202`; roles: dns-answer
- ipv4: `23.53.13.203`; roles: dns-answer, network-endpoint
- ipv4: `23.53.13.204`; roles: dns-answer
- ipv4: `23.53.13.205`; roles: dns-answer, network-endpoint
- ipv4: `23.53.13.206`; roles: dns-answer
- ipv4: `23.53.13.207`; roles: dns-answer
- ipv4: `23.53.13.208`; roles: dns-answer
- ipv4: `23.56.233.15`; roles: dns-answer, network-endpoint
- ipv4: `23.60.57.94`; roles: dns-answer, network-endpoint
- ipv4: `23.63.205.134`; roles: dns-answer, network-endpoint
- ipv4: `23.96.180.189`; roles: dns-answer, network-endpoint
- ipv4: `239.255.255.250`; roles: http-host, network-endpoint
- ipv4: `255.255.255.255`; roles: network-endpoint
- ipv4: `40.126.29.10`; roles: dns-answer, network-endpoint
- ipv4: `40.126.29.11`; roles: dns-answer
- ipv4: `40.126.29.12`; roles: dns-answer
- ipv4: `40.126.29.13`; roles: dns-answer, network-endpoint
- ipv4: `40.126.29.15`; roles: dns-answer
- ipv4: `40.126.29.5`; roles: dns-answer, network-endpoint
- ipv4: `40.126.29.6`; roles: dns-answer
- ipv4: `40.126.29.7`; roles: dns-answer
- ipv4: `40.126.29.8`; roles: dns-answer
- ipv4: `40.126.29.9`; roles: dns-answer
- ipv4: `51.116.253.170`; roles: dns-answer, network-endpoint
- ipv4: `52.109.0.136`; roles: dns-answer, network-endpoint
- ipv4: `52.109.0.142`; roles: dns-answer, network-endpoint
- ipv4: `52.109.20.38`; roles: dns-answer, network-endpoint
- ipv4: `52.113.194.132`; roles: dns-answer, network-endpoint
- ipv4: `52.123.128.254`; roles: dns-answer, network-endpoint
- ipv4: `52.123.129.254`; roles: dns-answer
- ipv4: `52.137.106.217`; roles: dns-answer, network-endpoint
- ipv4: `52.152.180.153`; roles: dns-answer, network-endpoint
- ipv4: `52.168.117.170`; roles: dns-answer, network-endpoint
- ipv4: `52.182.143.215`; roles: dns-answer, network-endpoint
- ipv4: `72.5.43.29`; roles: http-host, network-endpoint
- ja3: `08c552d3bb717cfa625b1c2e6293fbc3`; roles: tls-client-fingerprint
- ja3: `091f51a7a1c3a4504a224cc081ce9cee`; roles: tls-client-fingerprint
- ja3: `09218b185cad5bc9ac32dd4af1d80ba`; roles: tls-client-fingerprint
- ja3: `0940eef199c4e4a2d7fff1702ca8e267`; roles: tls-client-fingerprint
- ja3: `09d2a38ae19e8be7fa018ad87e43b2ff`; roles: tls-client-fingerprint
- ja3: `11156bf1dc969c54ae91bbfe52874a88`; roles: tls-client-fingerprint
- ja3: `11702f6f4b7b9c9b2999ebcf2c354984`; roles: tls-client-fingerprint
- ja3: `173448d57b47fba3f0be89e6bd4599af`; roles: tls-client-fingerprint
- ja3: `218b9f26907447fdbf2c8a52418444b7`; roles: tls-client-fingerprint
- ja3: `22833c8ba3c4d8d22ef4b3ff2fdd992e`; roles: tls-client-fingerprint
- ja3: `258a5a1e95b8a911872bae9081526644`; roles: tls-client-fingerprint
- ja3: `25e0b36f7a2832677e0c136c73a02311`; roles: tls-client-fingerprint
- ja3: `26abc27bb714c3e30049154ed7f03422`; roles: tls-client-fingerprint
- ja3: `2f7a1c53b0a1abfffcdeff101f69baf4`; roles: tls-client-fingerprint
- ja3: `33717d60eef91a9c824c343c9b904387`; roles: tls-client-fingerprint
- ja3: `34f7d1c3fe8b7bb4b8cee1ceefa986a5`; roles: tls-client-fingerprint
- ja3: `38ff17125ac547fdaf43cbc78d13056e`; roles: tls-client-fingerprint
- ja3: `3c293bdf2a25c07559b560ba86debc77`; roles: tls-client-fingerprint

```

- ja3: `3c4eb72b882d4d1442c67ce73f1292a9`; roles: tls-client-fingerprint
- ja3: `3ec074ef84f1118c439e56727227cea3`; roles: tls-client-fingerprint
- ja3: `46a78af27de56cd4c85b04f57deb3f79`; roles: tls-client-fingerprint
- ja3: `46f5131e766d248db0248a86c494b71c`; roles: tls-client-fingerprint
- ja3: `48ae6b908317f4f14e23cfd06798d78a`; roles: tls-client-fingerprint
- ja3: `49122e3f86717743d247b0e57255881e`; roles: tls-client-fingerprint
- ja3: `49a844a20d27ed5590377789c1ff9a1c`; roles: tls-client-fingerprint
- ja3: `4d09d5e0a7539f71bfd5ab61fc77938e`; roles: tls-client-fingerprint
- ja3: `4e00cf4e4608830803d4914864014e8c`; roles: tls-client-fingerprint
- ja3: `4e96df7dcbca32c279f0af5a0930aa87`; roles: tls-client-fingerprint
- ja3: `589c33f5c966de68b38bf824fc667e6b`; roles: tls-client-fingerprint
- ja3: `5919f6108f098e14c2f37619021ebd4d`; roles: tls-client-fingerprint
- ja3: `5c263245de4d50106d8e0d6087b0fcc5`; roles: tls-client-fingerprint
- ja3: `5c576ee905a82c07ad7987fce4f39cfe`; roles: tls-client-fingerprint
- ja3: `65005c9d9ae0f0ebeat22c210571d482`; roles: tls-client-fingerprint
- ja3: `68b1b54a6edfe7729708738380263a3a`; roles: tls-client-fingerprint
- ja3: `6925f81e11a98d706da3f0cd0f7bc648`; roles: tls-client-fingerprint
- ja3: `6a5d235ee78c6aede6a61448b4e9ff1e`; roles: tls-client-fingerprint
- ja3: `736a3b58b94abd6c394392ae94f501c3`; roles: tls-client-fingerprint
- ja3: `775ceba0b13f74a42447a14045d31fcc`; roles: tls-client-fingerprint
- ja3: `973e5ee0c53bfc4aaff964c70002dcc3`; roles: tls-client-fingerprint
- ja3: `a2fa4f21077551ea651d383707835d7b`; roles: tls-client-fingerprint
- ja3: `ab9d07f6268ed23da4f708263cc7ed49`; roles: tls-client-fingerprint
- ja3: `af8bdb53babad7f51a582d1ed25c0eda`; roles: tls-client-fingerprint
- ja3: `b1e1912cc21fd3c163c8ddf91f56123a`; roles: tls-client-fingerprint
- ja3: `b4162be74fb260b4576b62481ee819de`; roles: tls-client-fingerprint
- ja3: `b74979b1b06e1413e302d2c817ca33db`; roles: tls-client-fingerprint
- ja3: `b7e6d0a42505ebdcb4ca793e16825d04`; roles: tls-client-fingerprint
- ja3: `c44656a187a470fa1e85dfc1707da993`; roles: tls-client-fingerprint
- ja3: `c6e2484ca73f97e2cbb72bacc9c9916b`; roles: tls-client-fingerprint
- ja3: `cd51c3a587eeacaf4f714e3920764550`; roles: tls-client-fingerprint
- ja3: `d108c2f321a2af5781ed4b63b5b28472`; roles: tls-client-fingerprint
- ja3: `e978fa4306e6fe19e2d404321d215b00`; roles: tls-client-fingerprint
- ja3: `eb6eb038162eb12fda714a4a5860dc83`; roles: tls-client-fingerprint
- ja3: `ec93fbad48fbc839a6e52e85c3f5af8d`; roles: tls-client-fingerprint
- ja3: `f0a0d117d2207afbb65df9114a8c6321`; roles: tls-client-fingerprint
- ja3: `f957ed04f16c95c78f474482505d5e89`; roles: tls-client-fingerprint
- ja3: `fc2ac8b293f08f588c5b93dd8b87eef6`; roles: tls-client-fingerprint
- ja3: `fe624dd6795521519b6fbdbd082375f4f`; roles: tls-client-fingerprint
- sha256: `0078330840159b7adc1ec144a36905642a0469d68c4879febf76dbda26ffd5b2`; roles: exported-object
- sha256: `261daf6d8ef4a2ea145dbcd589a3808af3d734af40319248dbf81746bab0f594`; roles: exported-object
- sha256: `2ba81673f8cd827df283ad30f52bcaa0514fc065fef4398dafed3a0f612517f6`; roles: exported-object
- sha256: `41e87d5cfc89b6168dd794c2b32cdf83bff7fe164a603416d5d7d7e399109c9b`; roles: exported-object
- sha256: `5e4b21db2742377a82d65f7553eb8d183f781a561ff60f9421baee33b743fac4`; roles: exported-object
- sha256: `5e9a7996fe94d7be10595d7133748760bf8348198b71b7a50fd8affaa980ac61`; roles: exported-object
- sha256: `69bf0bc46f51b33377c4f3d92caf876714f6bbbe99e7544487327920873f9820`; roles: exported-object
- sha256: `6a42906135e357167d748aee9f36cb40fb5ba4584e85e7e1df4433ee8f38680c`; roles: exported-object
- sha256: `798563fcf7600f7ef1a35996291a9dfb5f9902733404dd499e2e736ea1dc6fc5`; roles: exported-object
- sha256: `8fcd6135214262cc9ef17efb67055b2a1baa9036a22325d8679192683c025e47`; roles: exported-object
- sha256: `9579dca191a7420bab906998ffd624709de7deda27481b53f6da693765f03499`; roles: exported-object
- sha256: `b7aec5f73d2a6bbd8cd920edb4760e2edadc98c3a45bf4fa994d47ca9cbd02f6`; roles: exported-object
- sha256: `be2882b8c36a2a65594e72f3cedb87b34523d2a8b13e23e902c4cd952a0a4252`; roles: exported-object
- sha256: `c54e6bd06d5c09a075e274a55c6d3ce31a2fabebbea38ce7083a9ebb7034a110`; roles: exported-object
- sha256: `dff7255b90139fbc8d3e76f31b480e65fc3eb7f49f70e7876cfb3f1cb56e5123`; roles: exported-object
- sha256: `f300d3238190768cae396cbc0263695abc1d8d2a1d9cf2b27bbd1a4d691ea64`; roles: exported-object
- sha256: `f394b14f8fb0b1d746f13e2acb5921e4c5962984836c1187147e341fcb693b0e`; roles: exported-object
- sha256: `f8313d5ec5090e37e52eef9455de8085810a8362db2e1226f3dc42f747651332`; roles: exported-object
- url: `http://239.255.255.250:1900*`; roles: http-request
- url: `http://72.5.43.29/`; roles: http-request
- url: `http://72.5.43.29/data/0f60a3e7baecf2748b1c8183ed37d1e4`; roles: http-request
- url: `http://acroipm2.adobe.com/assets/Owner/arm/ProcessMAU.txt`; roles: http-request
- url: `http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/8f2381c2-652d-48a2-86f6-19cb7757f5dc?P1=1724113284&P2=404&P3=2&P4=QwGPFdJVa%2bBw71q1beBnqYWDAtR86AnZ79I2%2fNOX9I1PkIMLSVOBKUK4QmaPqxVAgCpCijWyTVtZO9mpmuJNIQ%3d%3d`; roles: http-request
- url: `http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/f37dd878-a1b9-4f21-a8c9-65c3dd00f7a6?P1=1724225867&P2`

```

```

=404&P3=2&P4=laxXE3ikzdIKvQz1E1qPcLRRfyHtwqWgjEOYDO8CsvKt6Jcq94KnSHhjEOc1Vkk62%2budS1LrVl%2btTvm0Hctz%2bA%3d%3d`; roles: http-request
- url: `http://oneocsp.microsoft.com/ocsp/MFQwUjBQME4wTDAJBgUrDgMCGGUABBR2JNtr0JxEvYySpbyBWaqBmealCgQUzhUWO%2BoCo6Zr2tkr%2FeWMUr56UKGCEzMAPnPpacmgFoSqVQMAAAA%2Bc%2Bk%3D`; roles: http-request
- url: `http://quote.checkfedexexp.com/managements?16553a25e45250a41fd5&endeds=MIGpq&JStx=59bf050d37df88a9-ade43358-eea1220b-0571422b-0f33e6aa150e86bafd0ed4&Ld=9d7502d88d752a27b1d00587309184b5a215`; roles: http-request
- url: `http://www.msftconnecttest.com/connecttest.txt`; roles: http-request
- user_agent: `Microsoft BITS/7.8`; roles: http-client
- user_agent: `Microsoft Edge/127.0.2651.98 Windows`; roles: http-client
- user_agent: `Microsoft NCSI`; roles: http-client
- user_agent: `Microsoft-CryptoAPI/10.0`; roles: http-client
- user_agent: `Mozilla / 5.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705)`; roles: http-client
- user_agent: `Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)`; roles: http-client
- user_agent: `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36 Edg/127.0.0.0`; roles: http-client
- exported object `managements%3f16553a25e45250a41fd5&endeds=MIGpq&JStx=59bf050d37df88a9-ade43358-eea1220b-0571422b-0f33e6aa150e86bafd0ed4&Ld=9d7502d88d752a27b1d00587309184b5a215`; SHA-256 `798563fcf7600f7ef1a35996291a9dfb5f9902733404dd499e2e736ea1dc6fc5`; size 2767804 bytes
  Static content: `{"content_kind":"zip","features":[],"inspected_bytes":262144,"inspection_truncated":true,"interpretation":"Static content only; not proof of execution, intent, or malware family"}`. Not execution proof.
- exported object `0f60a3e7baecf2748b1c8183ed37d1e4`; SHA-256 `b7aec5f73d2a6bbd8cd920edb4760e2edadc98c3a45bf4fa994d47ca9cbd02f6`; size 159232 bytes
  Static content: `{"content_kind":"pe","features":[],"inspected_bytes":159232,"inspection_truncated":false,"interpretation":"Static content only; not proof of execution, intent, or malware family"}`. Not execution proof.
- exported object `%2f(3)`; SHA-256 `261daf6d8ef4a2ea145dbcd589a3808af3d734af40319248dbf81746bab0f594`; size 305148 bytes
- exported object `f37dd878-a1b9-4f21-a8c9-65c3dd00f7a6%3fP1=1724225867&P2=404&P3=2&P4=laxXE3ikzdIKvQz1E1qPcLRRfyHtwqWgjEOYDO8CsvKt6Jcq94KnSHhjEOc1Vkk62%2budS1LrVl%2btTvm0Hctz%2bA%3d%3d(3)`; SHA-256 `8fcd6135214262cc9ef17efb67055b2a1baa9036a22325d8679192683c025e47`; size 108543 bytes
- exported object `f37dd878-a1b9-4f21-a8c9-65c3dd00f7a6%3fP1=1724225867&P2=404&P3=2&P4=laxXE3ikzdIKvQz1E1qPcLRRfyHtwqWgjEOYDO8CsvKt6Jcq94KnSHhjEOc1Vkk62%2budS1LrVl%2btTvm0Hctz%2bA%3d%3d(2)`; SHA-256 `6a42906135e357167d748aee9f36cb40bf5ba4584e85e7e1df4433ee8f38680c`; size 29990 bytes
- exported object `f37dd878-a1b9-4f21-a8c9-65c3dd00f7a6%3fP1=1724225867&P2=404&P3=2&P4=laxXE3ikzdIKvQz1E1qPcLRRfyHtwqWgjEOYDO8CsvKt6Jcq94KnSHhjEOc1Vkk62%2budS1LrVl%2btTvm0Hctz%2bA%3d%3d`; SHA-256 `f8313d5ec5090e37e52eef9455de8085810a8362db2e1226f3dc42f747651332`; size 18882 bytes
- exported object `f37dd878-a1b9-4f21-a8c9-65c3dd00f7a6%3fP1=1724225867&P2=404&P3=2&P4=laxXE3ikzdIKvQz1E1qPcLRRfyHtwqWgjEOYDO8CsvKt6Jcq94KnSHhjEOc1Vkk62%2budS1LrVl%2btTvm0Hctz%2bA%3d%3d(1)`; SHA-256 `be2882b8c36a2a65594e72f3cedb87b34523d2a8b13e23e902c4cd952a0a4252`; size 13809 bytes
- exported object `8f2381c2-652d-48a2-86f6-19cb7757f5dc%3fP1=1724113284&P2=404&P3=2&P4=QwGPFdJVa%2bBw71q1beBnqYWdAtr86AnZ79l2%2fNOX9l1PkIMLSVOBKUK4QmaPqxVAgCpCljWyTvtZO9mpmuJNlIQ%3d%3d(3)`; SHA-256 `9579dca191a7420bab906998ffd624709de7deda27481b53f6da693765f03499`; size 7930 bytes
- exported object `8f2381c2-652d-48a2-86f6-19cb7757f5dc%3fP1=1724113284&P2=404&P3=2&P4=QwGPFdJVa%2bBw71q1beBnqYWdAtr86AnZ79l2%2fNOX9l1PkIMLSVOBKUK4QmaPqxVAgCpCljWyTvtZO9mpmuJNlIQ%3d%3d(2)`; SHA-256 `41e87d5cfc89b6168dd794c2b32cdf83bff7fe164a603416d5d7d7e399109c9b`; size 4630 bytes
- exported object `MFQwUjBQME4wTDAJBgUrDgMCGGUABBR2JNtr0JxEvYySpbyBWaqBmealCgQUzhUWO%2BoCo6Zr2tkr%2FeWMUr56UKGCEzMAPnPpacmgFoSqVQMAAAA%2Bc%2Bk%3D`; SHA-256 `2ba81673f8cd827df283ad30f52bcaa0514fc065fef4398dafed3a0f612517f6`; size 1782 bytes
- exported object `8f2381c2-652d-48a2-86f6-19cb7757f5dc%3fP1=1724113284&P2=404&P3=2&P4=QwGPFdJVa%2bBw71q1beBnqYWdAtr86AnZ79l2%2fNOX9l1PkIMLSVOBKUK4QmaPqxVAgCpCljWyTvtZO9mpmuJNlIQ%3d%3d(1)`; SHA-256 `0078330840159b7adc1ec144a36905642a0469d68c4879feb76dbda26ffd5b2`; size 1340 bytes
- exported object `8f2381c2-652d-48a2-86f6-19cb7757f5dc%3fP1=1724113284&P2=404&P3=2&P4=QwGPFdJVa%2bBw71q1beBnqYWdAtr86AnZ79l2%2fNOX9l1PkIMLSVOBKUK4QmaPqxVAgCpCljWyTvtZO9mpmuJNlIQ%3d%3d`; SHA-256 `c54e6bd06d5c09a075e274a55c6d3ce31a2fabebbea38ce7083a9ebb7034a110`; size 1120 bytes
- exported object `%2f(5)`; SHA-256 `f300d3238190768cae396cbc02636955abc1d8d2a1d9cf2b27bbd1a4d691ea64`; size 732 bytes
- exported object `%2f(1)`; SHA-256 `5e4b21db2742377a82d65f7553eb8d183f781a561ff60f9421baee33b743fac4`; size 124 bytes
- exported object `%2f(10)`; SHA-256 `f394b14f8fb0b1d746f13e2acb5921e4c5962984836c1187147e341fcb693b0e`; size 94 bytes
- exported object `%2f`; SHA-256 `dff7255b90139fbc8d3e76f31b480e65fc3eb7f49f70e7876cfb3f1cb56e5123`; size 32 bytes
- exported object `connecttest.txt`; SHA-256 `5e9a7996fe94d7be10595d7133748760bf8348198b71b7a50fd8affaa980ac61`; size 22 bytes
- exported object `ProcessMAU.txt`; SHA-256 `69bf0bc46f51b33377c4f3d92caf876714f6bbbe99e7544487327920873f9820`; size 4 bytes

```

Actor similarity leads

- Orangeworm (G0071): 50% TTP overlap. This is an investigation lead, not attribution.
- SilverTerrier (G0083): 25% TTP overlap. This is an investigation lead, not attribution.
- RedEcho (G1042): 20% TTP overlap. This is an investigation lead, not attribution.
- Metador (G1013): 11% TTP overlap. This is an investigation lead, not attribution.

- Rancor (G0075): 11% TTP overlap. This is an investigation lead, not attribution.
- APT18 (G0026): 8% TTP overlap. This is an investigation lead, not attribution.
- FIN4 (G0085): 8% TTP overlap. This is an investigation lead, not attribution.
- Dark Caracal (G0070): 8% TTP overlap. This is an investigation lead, not attribution.
- TA551 (G0127): 7% TTP overlap. This is an investigation lead, not attribution.
- BITTER (G1002): 6% 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: `d16753b47de8ecdb023abba50189bbcdcb68cf5a1d4b318a005b594ca7c48206`; recorded 2026-09-19T12:08:57.190731+00:00; mode: local-only.

Coverage: `{ "matched\_observables":0, "no\_exact\_match":272, "observable\_limit":5000, "observables\_checked":272, "observables\_total":272, "prior\_case\_limit\_reached":false, "prior\_cases\_checked":8, "truncated":false }`

- Catalog T1071.001: <https://attack.mitre.org/techniques/T1071/001>; detection strategies: [{ "attack_id":"DET0027", "name":"Detection of Web Protocol-Based C2 Over HTTP, HTTPS, or WebSockets", "stix_id":"x-mitre-detection-strategy--e6496b9b-2458-4616-9712-a7c0da7fd3bc" }]
- Prior analysis `faf041c3-70e0-4a01-8780-10917e5e187c` shares 42 observations. This does not establish a common campaign.
- Prior analysis `08324647-35af-4af2-8d82-4387eec03918` shares 46 observations. This does not establish a common campaign.
- Prior analysis `616a90fa-f15e-4fcb-8d56-7b8e0eff5785` shares 12 observations. This does not establish a common campaign.
- Prior analysis `459e119d-191f-49e8-85ea-c78f9de41826` shares 33 observations. This does not establish a common campaign.
- Prior analysis `7a2cfe72-f48d-4894-8a2d-8889cb3b11b2` shares 53 observations. This does not establish a common campaign.
- Prior analysis `81373b30-6a59-49d1-89b0-bad73ed19eaa` shares 37 observations. This does not establish a common campaign.
- Prior analysis `38851ad7-b3a0-423d-ae89-3b7be4e4b908` shares 36 observations. This does not establish a common campaign.
- Prior analysis `bfccc426-aa9b-4007-8558-a66d37ecb90c` shares 69 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":18, "exported_objects":322, "hashed_bytes":3449794, "hashed_objects":322, "omitted_unique_hashes":0, "returned_unique_hashes":18, "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":18 }`. 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 8/8, identities 5/5, observables 272/272, artifacts 18/18. Full returned inventory is in the JSON result.