

AdversaryGraph

Threat Intelligence Analysis Report

Analysis Metadata

Provider:	deterministic
Model:	tshark-evidence-v3
Domain:	enterprise-attack
Session ID:	426471ed-5e63-4b7e-ac6c-d36e060a4739
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 26922 packets across 61 IP endpoints and 276 transport flows. Observed 343 DNS events, 74 HTTP requests, 109 TLS ClientHello events, and 11 exported HTTP object(s). Deterministic rules produced 12 finding(s): 2 high, 2 medium, and 8 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: 28778 / 28778 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	pass	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:202
- 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: 2024-11-26-traffic-analysis-exercise.pcap

Capture SHA-256: `a38267943a7bf3b0e445d7e51cb0a68b3dee797d67081bc9a033f73d079c0f50`

Semantic result SHA-256: `4fa4f2aabaa7bcc51a396dcd62fc65dbd2ee862d01d0ba16095da5915212d518`

Analyzer manifest SHA-256: `ee952aeb7cdc6958f4ae5178c54c274a1e4f0aec4d42f3bdb95baaff063b3dde`

Executive summary

Decoded 26922 packets across 61 IP endpoints and 276 transport flows. Observed 343 DNS events, 74 HTTP requests, 109 TLS ClientHello events, and 11 exported HTTP object(s). Deterministic rules produced 12 finding(s): 2 high, 2 medium, and 8 low. Findings are evidence-bound candidates and require analyst review; encrypted payload contents remain unavailable.

Capture facts

- Packets: 26922
- Duration: 3259.651349 seconds
- Captured bytes: 20851149
- Endpoints: 61
- Flows: 276

Deterministic findings

MEDIUM \u2014 Cleartext HTTP observed on TCP/443

The decoded application protocol is HTTP despite use of the conventional TLS port.

Rule: `http-on-tls-port@pcap-rules-v3`; confidence: 0.98; evidence: frame 20340 / TCP stream 77, frame 20342 / TCP stream 77, frame 20348 / TCP stream 77, frame 20350 / TCP stream 77, frame 20572 / TCP stream 77.

Metrics: `{\"destination\":\"194.180.191.64\",\"host\":\"194.180.191.64\",\"request\_count\":58,\"source\":\"10.11.26.183\",\"uri\":\"http://194.180.191.64/fakeurl.htm\"}`

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 20340 / TCP stream 77, frame 20342 / TCP stream 77, frame 20348 / TCP stream 77, frame 20350 / TCP stream 77, frame 20572 / TCP stream 77.

Metrics: `{\"destination\":\"194.180.191.64\",\"host\":\"194.180.191.64\",\"median\_absolute\_deviation\":0.091,\"median\_interval\_seconds\":60.154,\"method\":\"POST\",\"port\":443,\"request\_count\":58,\"source\":\"10.11.26.183\",\"uri\":\"http://194.180.191.64/fakeurl.htm\"}`

HIGH \u2014 Remote-access software network signature

An HTTP User-Agent explicitly identifies remote-access software. Validate authorization and endpoint ownership.

Rule: `remote-access-user-agent@pcap-rules-v3`; confidence: 0.95; evidence: frame 20340 / TCP stream 77, frame 20342 / TCP stream 77, frame 20348 / TCP stream 77, frame 20350 / TCP stream 77, frame 20572 / TCP stream 77.

Metrics: `{\"destination\":\"194.180.191.64\",\"request\_count\":58,\"source\":\"10.11.26.183\",\"user\_agent\":\"NetSupport Manager/1.3\"}`

MEDIUM \u2014 Repeated outbound HTTP POST activity

The same endpoint pair and HTTP target produced repeated POST requests suitable for beaconing or data transfer review.

Rule: `repeated-http-posts@pcap-rules-v3`; confidence: 0.72; evidence: frame 20340 / TCP stream 77, frame 20342 / TCP stream 77, frame 20348 / TCP stream 77, frame 20350 / TCP stream 77, frame 20572 / TCP stream 77.

Metrics: `{"declared\_body\_bytes":2624,"destination":"194.180.191.64","host":"194.180.191.64","port":443,"request\_count":58,"source":"10.11.26.183","url":"http://194.180.191.64/fakeurl.htm"}`

LOW 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 23, frame 25, frame 189, frame 190, frame 902.

Metrics: `{"domain":"wpad.mshome.net","response\_count":24,"source":"10.11.26.183"}`

LOW 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 20, frame 185, frame 186, frame 898.

Metrics: `{"domain":"wpad.nemotoads.health","response\_count":24,"source":"10.11.26.183"}`

LOW 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 304 / TCP stream 11, frame 309 / TCP stream 11, frame 312 / TCP stream 11, frame 315 / TCP stream 11, frame 486 / TCP stream 24.

Metrics: `{"destination":"10.11.26.3","event\_count":25,"operation\_numbers":["0","1","12"],"protocol":"drsuapi","source":"10.11.26.183"}`

LOW 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 36 / TCP stream 1, frame 43 / TCP stream 1, frame 46 / TCP stream 1, frame 359 / TCP stream 16, frame 371 / TCP stream 16.

Metrics: `{"destination":"10.11.26.3","event\_count":64,"operation\_numbers":["","0","2","3"],"protocol":"ldap","source":"10.11.26.183"}`

LOW 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 330 / TCP stream 10, frame 334 / TCP stream 10, frame 340 / TCP stream 10, frame 344 / TCP stream 10, frame 346 / TCP stream 10.

Metrics: `{"destination":"10.11.26.3","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"10.11.26.183"}`

LOW 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 305 / TCP stream 11, frame 311 / TCP stream 11, frame 313 / TCP stream 11, frame 316 / TCP stream 11, frame 487 / TCP stream 24.

Metrics: `{"destination":"10.11.26.183","event\_count":25,"operation\_numbers":["0","1","12"],"protocol":"drsuapi","source":"10.11.26.3"}`

LOW 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 40 / TCP stream 1, frame 45 / TCP stream 1, frame 363 / TCP stream 16, frame 379 / TCP stream 16, frame 383 / TCP stream 16.

Metrics: `{ "destination": "10.11.26.183", "event\_count": 49, "operation\_numbers": [ "1", "4", "19", "19", "19", "5", "4", "5", "5" ], "protocol": "ldap", "source": "10.11.26.3" }`

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 333 / TCP stream 10, frame 337 / TCP stream 10, frame 342 / TCP stream 10, frame 345 / TCP stream 10, frame 348 / TCP stream 10.

Metrics: `{ "destination": "10.11.26.183", "event\_count": 15, "operation\_numbers": [ "1", "16", "17", "3", "34", "36", "39", "5", "6", "64", "7" ], "protocol": "samr", "source": "10.11.26.3" }`

ATT&CK candidates

- T1071.001 Application Layer Protocol: Web Protocols (command-and-control), confidence=0.85, status=suggested; basis=versioned-deterministic-rule.
- T1219 Remote Access Software (command-and-control), confidence=0.9, status=suggested; basis=versioned-deterministic-rule.

Identities

- account: `oboomwald`; client IPs: 10.11.26.183; frames: 213, 221, 223, 235, 275
- full-name: `Oliver Q. Boomwald`; client IPs: 10.11.26.183; frames: 355
- hostname: `DESKTOP-B8TQK49`; client IPs: 10.11.26.183; frames: 69, 70, 145, 146, 174
- netbios-group: `NEMOTODES`; client IPs: unbound subject; frames: 71, 144, 176, 180, 191

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: `armmf.adobe.com`; roles: dns-query, tls-sni
- domain: `assets.msn.com`; roles: dns-query, tls-sni
- domain: `checkappexec.microsoft.com`; roles: dns-query, tls-sni
- domain: `classicgrand.com`; roles: dns-query, tls-sni
- domain: `client.wns.windows.com`; roles: dns-query, tls-sni
- domain: `code.jquery.com`; roles: dns-query, tls-sni
- domain: `confirmsubscription.com`; roles: dns-query, tls-sni
- domain: `css.createzend1.com`; roles: dns-query, tls-sni
- domain: `ctdl.windowsupdate.com`; roles: dns-query, http-host
- domain: `d33w6v2v5ta015.cloudfront.net`; roles: dns-cname
- domain: `data-edge.smartscreen.microsoft.com`; 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: `dns.msftncsi.com`; roles: dns-query
- domain: `ecs.office.com`; 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: `fa000000002.resources.office.net`; roles: dns-query, tls-sni
- domain: `fa000000005.resources.office.net`; roles: dns-query, tls-sni
- domain: `fa000000116.resources.office.net`; roles: dns-query, tls-sni
- domain: `fa000000128.resources.office.net`; roles: dns-query, tls-sni
- domain: `fa000000163.resources.office.net`; roles: dns-query, tls-sni
- domain: `fd.api.iris.microsoft.com`; roles: dns-query, tls-sni
- domain: `fe3cr.delivery.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `fonts.googleapis.com`; roles: dns-query, tls-sni
- domain: `fonts.gstatic.com`; roles: dns-query, tls-sni
- domain: `geo.netsupportsoftware.com`; roles: dns-query, http-host
- domain: `img-s-msn-com.akamaized.net`; roles: dns-query, tls-sni

- domain: `inputsuggestions.msdxcdn.microsoft.com`; roles: dns-query, tls-sni
- domain: `js.createsend1.com`; roles: dns-query, tls-sni
- domain: `licensing.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `login.live.com`; roles: dns-query, tls-sni
- domain: `login.microsoftonline.com`; roles: tls-sni
- domain: `maps.googleapis.com`; roles: dns-query, tls-sni
- domain: `maps.gstatic.com`; roles: dns-query, tls-sni
- domain: `mobile.events.data.microsoft.com`; roles: dns-query, tls-sni
- domain: `modandcrackedapk.com`; roles: dns-query, tls-sni
- domain: `mrodevicemgr.officeapps.live.com`; roles: dns-query, tls-sni
- domain: `nav.smartscreen.microsoft.com`; roles: dns-query, tls-sni
- domain: `nemotodes-dc.nemotoads.health`; roles: dns-query
- domain: `odc.officeapps.live.com`; roles: dns-query, tls-sni
- domain: `officeclient.microsoft.com`; roles: dns-query, tls-sni
- domain: `prod.mrodevicemgr.live.com.akadns.net`; roles: dns-cname
- domain: `r10.o.lencr.org`; roles: dns-query, http-host
- 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: `windows.msn.com`; roles: dns-query, tls-sni
- domain: `wns.notify.trafficmanager.net`; roles: dns-cname
- domain: `wpad.mshome.net`; roles: dns-query
- domain: `wpad.nemotoads.health`; roles: dns-query
- domain: `www.bing.com`; roles: dns-query, tls-sni
- domain: `www.google.com`; roles: dns-query, tls-sni
- domain: `www.gstatic.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: `10.11.26.183`; roles: network-endpoint
- ipv4: `10.11.26.255`; roles: network-endpoint
- ipv4: `10.11.26.3`; roles: dns-answer, network-endpoint
- ipv4: `104.117.244.104`; roles: dns-answer
- ipv4: `104.117.244.105`; roles: dns-answer, network-endpoint
- ipv4: `104.117.244.106`; roles: dns-answer, network-endpoint
- ipv4: `104.117.244.107`; roles: dns-answer
- ipv4: `104.117.244.112`; roles: dns-answer, network-endpoint
- ipv4: `104.117.244.114`; roles: dns-answer
- ipv4: `104.117.244.72`; roles: dns-answer
- ipv4: `104.117.244.74`; roles: dns-answer
- ipv4: `104.117.244.81`; roles: dns-answer
- ipv4: `104.117.244.82`; roles: dns-answer
- ipv4: `104.117.244.88`; roles: dns-answer
- ipv4: `104.117.244.89`; roles: dns-answer
- ipv4: `104.117.244.91`; roles: dns-answer
- ipv4: `104.117.244.96`; roles: dns-answer, network-endpoint
- ipv4: `104.117.244.97`; roles: dns-answer
- ipv4: `104.117.244.99`; roles: dns-answer
- ipv4: `104.117.247.139`; roles: dns-answer
- ipv4: `104.117.247.144`; roles: dns-answer
- ipv4: `104.117.247.162`; roles: dns-answer, network-endpoint
- ipv4: `104.117.247.184`; roles: dns-answer, network-endpoint
- ipv4: `104.117.247.186`; roles: dns-answer
- ipv4: `104.117.247.67`; roles: dns-answer
- ipv4: `104.117.247.99`; roles: dns-answer, network-endpoint
- ipv4: `104.26.0.231`; roles: dns-answer
- ipv4: `104.26.1.231`; 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: `13.107.5.93`; roles: dns-answer, network-endpoint
- ipv4: `13.56.30.207`; roles: dns-answer, network-endpoint
- ipv4: `131.107.255.255`; roles: dns-answer
- ipv4: `142.250.113.120`; roles: dns-answer, network-endpoint
- ipv4: `142.250.113.94`; roles: dns-answer, network-endpoint
- ipv4: `142.250.113.95`; roles: dns-answer

- ipv4: `142.250.114.95`; roles: dns-answer
- ipv4: `142.250.115.95`; roles: dns-answer, network-endpoint
- ipv4: `142.250.138.94`; roles: dns-answer, network-endpoint
- ipv4: `142.251.116.95`; roles: dns-answer
- ipv4: `142.251.186.103`; roles: dns-answer
- ipv4: `142.251.186.104`; roles: dns-answer
- ipv4: `142.251.186.105`; roles: dns-answer
- ipv4: `142.251.186.106`; roles: dns-answer
- ipv4: `142.251.186.147`; roles: dns-answer, network-endpoint
- ipv4: `142.251.186.95`; roles: dns-answer, network-endpoint
- ipv4: `142.251.186.99`; roles: dns-answer
- ipv4: `151.101.130.137`; roles: dns-answer
- ipv4: `151.101.194.137`; roles: dns-answer
- ipv4: `151.101.2.137`; roles: dns-answer
- ipv4: `151.101.66.137`; roles: dns-answer, network-endpoint
- ipv4: `172.67.68.212`; roles: dns-answer
- ipv4: `173.222.49.101`; roles: dns-answer, network-endpoint
- ipv4: `18.160.156.103`; roles: dns-answer, network-endpoint
- ipv4: `18.160.156.61`; roles: dns-answer, network-endpoint
- ipv4: `18.160.156.77`; roles: dns-answer
- ipv4: `18.160.156.92`; roles: dns-answer
- ipv4: `193.42.38.139`; roles: dns-answer, network-endpoint
- ipv4: `194.180.191.64`; roles: http-host, network-endpoint
- ipv4: `20.189.173.16`; roles: dns-answer, network-endpoint
- ipv4: `20.189.173.23`; roles: dns-answer, network-endpoint
- ipv4: `20.189.173.26`; roles: dns-answer, network-endpoint
- ipv4: `20.189.173.6`; roles: dns-answer, network-endpoint
- ipv4: `20.190.135.2`; roles: dns-answer
- ipv4: `20.190.135.3`; roles: dns-answer
- ipv4: `20.190.135.6`; roles: dns-answer
- ipv4: `20.190.135.7`; roles: dns-answer
- ipv4: `20.42.73.25`; roles: dns-answer, network-endpoint
- ipv4: `20.42.73.28`; roles: dns-answer, network-endpoint
- ipv4: `20.7.1.246`; roles: dns-answer, network-endpoint
- ipv4: `20.7.2.167`; 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: `204.79.197.239`; roles: dns-answer, network-endpoint
- ipv4: `213.246.109.5`; roles: dns-answer, network-endpoint
- ipv4: `224.0.0.251`; roles: network-endpoint
- ipv4: `224.0.0.252`; roles: network-endpoint
- ipv4: `23.201.68.167`; roles: dns-answer, network-endpoint
- ipv4: `23.204.171.61`; roles: dns-answer, network-endpoint
- ipv4: `23.219.87.81`; roles: dns-answer
- ipv4: `23.221.22.196`; roles: dns-answer
- ipv4: `23.221.22.205`; roles: dns-answer
- ipv4: `23.221.22.206`; roles: dns-answer
- ipv4: `23.221.22.207`; roles: dns-answer
- ipv4: `23.221.22.208`; roles: dns-answer
- ipv4: `23.221.22.209`; roles: dns-answer, network-endpoint
- ipv4: `23.221.22.217`; roles: dns-answer
- ipv4: `23.221.22.218`; roles: dns-answer
- ipv4: `23.221.22.219`; roles: dns-answer
- ipv4: `23.221.22.46`; roles: dns-answer, network-endpoint
- ipv4: `23.221.22.57`; roles: dns-answer
- ipv4: `23.53.127.105`; roles: dns-answer, network-endpoint
- ipv4: `23.53.127.114`; roles: dns-answer
- ipv4: `23.53.127.200`; roles: dns-answer, network-endpoint
- ipv4: `239.255.255.250`; roles: http-host, network-endpoint
- ipv4: `4.149.227.78`; roles: dns-answer, network-endpoint
- ipv4: `4.150.155.223`; roles: dns-answer, network-endpoint
- ipv4: `40.118.171.167`; roles: dns-answer, network-endpoint
- ipv4: `40.126.28.11`; roles: dns-answer, network-endpoint
- ipv4: `40.126.28.14`; roles: dns-answer

- ipv4: `40.126.28.22`; roles: dns-answer
- ipv4: `40.126.29.9`; roles: network-endpoint
- ipv4: `40.126.7.32`; roles: dns-answer
- ipv4: `52.109.0.136`; roles: dns-answer, network-endpoint
- ipv4: `52.109.20.47`; roles: dns-answer, network-endpoint
- ipv4: `52.109.8.89`; roles: dns-answer, network-endpoint
- ipv4: `52.113.194.132`; roles: dns-answer, network-endpoint
- ipv4: `52.165.164.15`; roles: dns-answer, network-endpoint
- ipv4: `52.168.112.67`; roles: dns-answer, network-endpoint
- ipv4: `52.8.34.0`; roles: dns-answer, network-endpoint
- ja3: `0652c09be13a164e73c3c66e2d5cd600`; roles: tls-client-fingerprint
- ja3: `089117d8abb9d0685ac2756412f44d8c`; roles: tls-client-fingerprint
- ja3: `091f51a7a1c3a4504a224cc081ce9cee`; roles: tls-client-fingerprint
- ja3: `0d7e324cc471d537395a5a84963ff4c0`; roles: tls-client-fingerprint
- ja3: `10b3abe91219287930575e96187aab46`; roles: tls-client-fingerprint
- ja3: `129a4a4460936a7d35cf0b4a876c02c5`; roles: tls-client-fingerprint
- ja3: `1a41c18f74e0a1125e7eb86dc20da423`; roles: tls-client-fingerprint
- ja3: `1aef2a0442d1535b67c961be49fbd9b0`; roles: tls-client-fingerprint
- ja3: `1d2c110dc93a519d4c14a15898f20f6c`; roles: tls-client-fingerprint
- ja3: `258a5a1e95b8a911872bae9081526644`; roles: tls-client-fingerprint
- ja3: `2800f914a7a4ba98aa9df62d316a460c`; roles: tls-client-fingerprint
- ja3: `2dd32544ddd46095f157e79a028dcda9`; roles: tls-client-fingerprint
- ja3: `2ef63960b5419ce0be770acb72a1e6d5`; roles: tls-client-fingerprint
- ja3: `34578b889dbdf86b5a0639eb869f9c5`; roles: tls-client-fingerprint
- ja3: `39a2db8b2473a3d4cfe7cb23a26e03d6`; roles: tls-client-fingerprint
- ja3: `46181092bc7467ccd870ec99523f7113`; roles: tls-client-fingerprint
- ja3: `488f29e13a0873e296eb2dcca6ec38d0`; roles: tls-client-fingerprint
- ja3: `4c24b4903c9a3c9b3c46306472bda896`; roles: tls-client-fingerprint
- ja3: `53e42f80bc48a39739f5221b803b1f70`; roles: tls-client-fingerprint
- ja3: `5c0851e1f7c97a5fdf8ee34bd73a8ff4`; roles: tls-client-fingerprint
- ja3: `6634ba84945fce7cc2d7864edc49b103`; roles: tls-client-fingerprint
- ja3: `68b3ecfaf0034bb9fcbecd518b5ab8d4`; roles: tls-client-fingerprint
- ja3: `6a5d235ee78c6aede6a61448b4e9ff1e`; roles: tls-client-fingerprint
- ja3: `7117eb033929b913d5dbbef620c9ca24`; roles: tls-client-fingerprint
- ja3: `7230db75fdb5472f76d02c10787af505`; roles: tls-client-fingerprint
- ja3: `82fc3feb7b73141563a581cb3a02b9e2`; roles: tls-client-fingerprint
- ja3: `893fda16143345fbd7d6384fd5f69a44`; roles: tls-client-fingerprint
- ja3: `8f08a45cb17ce5d331bb4a861f26181f`; roles: tls-client-fingerprint
- ja3: `910d5ef16eeb9c556a6f011876c16d38`; roles: tls-client-fingerprint
- ja3: `9763df22d3de0549862e28d0f1103365`; roles: tls-client-fingerprint
- ja3: `97cdfdfb6ce55b090e5070647c73305e`; roles: tls-client-fingerprint
- ja3: `996d810fbaded0fd221205ee7a391364`; roles: tls-client-fingerprint
- ja3: `9c5ffd0e64cc58a2ad1806964fe2da4e`; roles: tls-client-fingerprint
- ja3: `a702db92a1dad8b0a7ddf9ef0fc3d68`; roles: tls-client-fingerprint
- ja3: `ab617a1bfb55ac132b8893703d7cfec3`; roles: tls-client-fingerprint
- ja3: `af5ca235cbec16c4b5ad43da2bd9b40a`; roles: tls-client-fingerprint
- ja3: `b13922eb23a33bd76cd8442814f25cb5`; roles: tls-client-fingerprint
- ja3: `b6b910fa2621ea444621910f5e10aa4a`; roles: tls-client-fingerprint
- ja3: `b8f7a95293e0d02d297ecef1efcc79d5`; roles: tls-client-fingerprint
- ja3: `c73376907efd66947a8978eacfd15135`; roles: tls-client-fingerprint
- ja3: `c806504b9d641f3b26d1af269ed474ab`; roles: tls-client-fingerprint
- ja3: `c86423ffed1add9d50ccf646bd7fdbd`; roles: tls-client-fingerprint
- ja3: `cbcf96af03d431db8e0fd90215b03309`; roles: tls-client-fingerprint
- ja3: `d7268fba5c8ebdc86121861931c04402`; roles: tls-client-fingerprint
- ja3: `e544273138fcf6e7dc137dd4f74d6fd0`; roles: tls-client-fingerprint
- ja3: `e71e6cff682837413473fd63dc10f5d4`; roles: tls-client-fingerprint
- ja3: `f24a7ea8a60779966dc83806405c4091`; roles: tls-client-fingerprint
- ja3: `f82158b828f02d82f1f70fbb0f1d6145`; roles: tls-client-fingerprint
- ja3: `fae0e5d973c96ae1888b99538efa0363`; roles: tls-client-fingerprint
- sha256: `2b69346572041eefe558a82b58d654237e087ce9ab4e0876254a40a8954279a9`; roles: exported-object
- sha256: `59dc18363d5d0313ae94aa0ecad2d06dc77144758eeae2cc5ed8b4eee3923752`; roles: exported-object
- sha256: `5e9a7996fe94d7be10595d7133748760bf8348198b71b7a50fd8affaa980ac61`; roles: exported-object
- sha256: `69bf0bc46f51b33377c4f3d92caf876714f6bbbe99e7544487327920873f9820`; roles: exported-object
- sha256: `79653567106d923034d36a9025d2d37955ff55dae5d77c1a79a321d850235d00`; roles: exported-object
- sha256: `839e234a3a10b60d559ee5679d2019ad4e58d9cd66e6cfd971207c3c6ef8ea4d`; roles: exported-object

```

- sha256: `975b5678560775735da4a9e8b805dce370329179b8e17ebc1c289aaeb293f7ff`; roles: exported-object
- sha256: `a5a0a597e4b76ebec517a83126dbce37625a763b57307afe7064d9eb0a523956`; roles: exported-object
- sha256: `af0c1c32558e6dc1e4e8f3e1d151268b8f6eb7cd844c9ac6dfc4b862decc7983`; roles: exported-object
- sha256: `cd6f72bd96cbbad446325f8c2d087283f051ccaf77523dc436eec2d98be29bf7`; roles: exported-object
- sha256: `f0e200cadc273e3dd257057f27aeda839a1f2f31482e0bb01ea8b1363a7af245`; roles: exported-object
- url: `http://194.180.191.64/fakeurl.htm`; roles: http-request
- url: `http://239.255.255.250:1900*`; roles: http-request
- url: `http://acroipm2.adobe.com/assets/Owner/arm/ProcessMAU.txt`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?7778a0928305752e9`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?ce02e9976e1239e1`; roles: http-request
- url: `http://geo.netsupportsoftware.com/location/loca.asp`; roles: http-request
- url: `http://r10.o.lencr.org/MFMwUTBPME0wSzAJBgUrDgMCGGUABBRpD%2BQVZ%2B1vf7U0RGQGBm8JZwdxcgQUdKR2KRcYVIUxN75n5gZYwLzFBXICEgRSsdGCXQJkIJZNBHi669GH4A%3D%3D`; roles: http-request
- url: `http://www.msftconnecttest.com/connecttest.txt`; roles: http-request
- user_agent: `Microsoft NCSI`; roles: http-client
- user_agent: `Microsoft-CryptoAPI/10.0`; roles: http-client
- user_agent: `Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Tablet PC 2.0)`; roles: http-client
- user_agent: `NetSupport Manager/1.3`; roles: http-client
- exported object `MFMwUTBPME0wSzAJBgUrDgMCGGUABBRpD%2BQVZ%2B1vf7U0RGQGBm8JZwdxcgQUdKR2KRcYVIUxN75n5gZYwLzFBXICEgRSsdGCXQJkIJZNBHi669GH4A%3D%3D`; SHA-256 `cd6f72bd96cbbad446325f8c2d087283f051ccaf77523dc436eec2d98be29bf7`; size 504 bytes
- exported object `fakeurl(2).htm`; SHA-256 `839e234a3a10b60d559ee5679d2019ad4e58d9cd66e6cfd971207c3c6ef8ea4d`; size 250 bytes
- exported object `fakeurl(3).htm`; SHA-256 `a5a0a597e4b76ebec517a83126dbce37625a763b57307afe7064d9eb0a523956`; size 152 bytes
- exported object `fakeurl(5).htm`; SHA-256 `59dc18363d5d0313ae94aa0ecad2d06dc77144758eeae2cc5ed8b4eee3923752`; size 84 bytes
- exported object `fakeurl(4).htm`; SHA-256 `f0e200cadc273e3dd257057f27aeda839a1f2f31482e0bb01ea8b1363a7af245`; size 76 bytes
- exported object `fakeurl(1).htm`; SHA-256 `79653567106d923034d36a9025d2d37955ff55dae5d77c1a79a321d850235d00`; size 61 bytes
- exported object `fakeurl(10).htm`; SHA-256 `975b5678560775735da4a9e8b805dce370329179b8e17ebc1c289aaeb293f7ff`; size 36 bytes
- exported object `fakeurl(54).htm`; SHA-256 `2b69346572041eeef558a82b58d654237e087ce9ab4e0876254a40a8954279a9`; size 22 bytes
- exported object `connecttest.txt`; SHA-256 `5e9a7996fe94d7be10595d7133748760bf8348198b71b7a50fd8affaa980ac61`; size 22 bytes
- exported object `loca.asp`; SHA-256 `af0c1c32558e6dc1e4e8f3e1d151268b8f6eb7cd844c9ac6dfc4b862decc7983`; size 16 bytes
- exported object `ProcessMAU.txt`; SHA-256 `69bf0bc46f51b33377c4f3d92caf876714f6bbbe99e7544487327920873f9820`; size 4 bytes

```

Actor similarity leads

- Orangeworm (G0071): 33% TTP overlap. This is an investigation lead, not attribution.
- SilverTerrier (G0083): 20% TTP overlap. This is an investigation lead, not attribution.
- RedEcho (G1042): 17% TTP overlap. This is an investigation lead, not attribution.
- Carbanak (G0008): 10% TTP overlap. This is an investigation lead, not attribution.
- Metador (G1013): 10% TTP overlap. This is an investigation lead, not attribution.
- GOLD SOUTHFIELD (G0115): 10% TTP overlap. This is an investigation lead, not attribution.
- Rancor (G0075): 10% TTP overlap. This is an investigation lead, not attribution.
- DarkVishnya (G0105): 9% 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.

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: `82f0a542eadbd91c1d0554cf45b8bd4f69607e372cf96649bcd6ec9cab5fafb8`; recorded 2026-09-19T12:08:41.573203+00:00; mode: local-only.

Coverage: `{"matched\_observables":0,"no\_exact\_match":243,"observable\_limit":5000,"observables\_checked":243,"observables\_total":243,"prior\_case\_limit\_reached":false,"prior\_cases\_checked":6,"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"}]
- Catalog T1219: <https://attack.mitre.org/techniques/T1219>; detection strategies: [{"attack_id":"DET0496","name":"Behavior-Chain Detection for Remote Access Tools (Tool-Agnostic)","stix_id":"x-mitre-detection-strategy--ec412019-109f-4f84-aa2f-d623f40254e0"}]
- Prior analysis `616a90fa-f15e-4fcb-8d56-7b8e0eff5785` shares 10 observations. This does not establish a common campaign.
- Prior analysis `459e119d-191f-49e8-85ea-c78f9de41826` shares 30 observations. This does not establish a common campaign.
- Prior analysis `7a2cfe72-f48d-4894-8a2d-8889cb3b11b2` shares 46 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 37 observations. This does not establish a common campaign.
- Prior analysis `bfcc426-aa9b-4007-8558-a66d37ecb90c` shares 54 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": 11, "exported_objects": 66, "hashed_bytes": 3596, "hashed_objects": 66, "omitted_unique_hashes": 0, "returned_unique_hashes": 11, "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": 11 }`. 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 12/12, identities 4/4, observables 243/243, artifacts 11/11. Full returned inventory is in the JSON result.