

AdversaryGraph

Threat Intelligence Analysis Report

Analysis Metadata

Provider:	deterministic
Model:	tshark-evidence-v3
Domain:	enterprise-attack
Session ID:	2b5677d6-f466-4831-89aa-be3126dddaef
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 84542 packets across 216 IP endpoints and 2746 transport flows. Observed 2061 DNS events, 120 HTTP requests, 409 TLS ClientHello events, and 4 exported HTTP object(s). Deterministic rules produced 37 finding(s): 0 high, 13 medium, and 24 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 / 55549 characters
Promotion ready: No

#	Gate	Machine	Analyst	Reason
1	Source provenance	warning	pending	
2	Publication date	fail	pending	
3	Procedure relevance	fail	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:200
- 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: 2021-10-22-ISC-forensic-challenge-traffic.pcap

Capture SHA-256: `95074aea864749524df5b0a6c9fd58a3111038157b3400902486b96d902b3455`

Semantic result SHA-256: `e2a781b6839946af3b4581e8fbba850bc68bbe393fce12f786178323e0ccd04d`

Analyzer manifest SHA-256: `ee952aeb7cdc6958f4ae5178c54c274a1e4f0aec4d42f3bdb95baaff063b3dde`

Executive summary

Decoded 84542 packets across 216 IP endpoints and 2746 transport flows. Observed 2061 DNS events, 120 HTTP requests, 409 TLS ClientHello events, and 4 exported HTTP object(s). Deterministic rules produced 37 finding(s): 0 high, 13 medium, and 24 low. Findings are evidence-based and candidates and require analyst review; encrypted payload contents remain unavailable.

Capture facts

- Packets: 84542
- Duration: 5547.683987 seconds
- Captured bytes: 47654732
- Endpoints: 216
- Flows: 2746

Deterministic findings

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 825, frame 1639, frame 2954, frame 15029, frame 17432.

Metrics: `{\"domain\":\"wpad.enemywatch.net\",\"response\_count\":42,\"source\":\"10.10.22.156\"}`

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 827, frame 1641, frame 2956, frame 15031, frame 17435.

Metrics: `{\"domain\":\"wpad.localdomain\",\"response\_count\":42,\"source\":\"10.10.22.156\"}`

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 39, frame 752, frame 1643, frame 11964, frame 22840.

Metrics: `{\"domain\":\"wpad.enemywatch.net\",\"response\_count\":12,\"source\":\"10.10.22.157\"}`

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 41, frame 754, frame 1645, frame 11966, frame 22842.

Metrics: `{\"domain\":\"wpad.localdomain\",\"response\_count\":12,\"source\":\"10.10.22.157\"}`

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 1719, frame 2522, frame 3813, frame 6217, frame 6501.

Metrics: `{"domain":"wpad.enemywatch.net","response\_count":16,"source":"10.10.22.158"}`

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 1721, frame 2524, frame 3815, frame 6219, frame 6503.

Metrics: `{"domain":"wpad.localdomain","response\_count":16,"source":"10.10.22.158"}`

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 999 / TCP stream 46, frame 1001 / TCP stream 46, frame 1003 / TCP stream 46, frame 1013 / TCP stream 46, frame 1015 / TCP stream 46.

Metrics: `{"destination":"10.10.22.22","event\_count":59,"operation\_numbers":["0","1","12","13","30"],"protocol":"drsuapi","source":"10.10.22.156"}`

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 804 / TCP stream 37, frame 965 / TCP stream 37, frame 994 / TCP stream 37, frame 1062 / TCP stream 55, frame 1069 / TCP stream 55.

Metrics: `{"destination":"10.10.22.22","event\_count":102,"operation\_numbers":["","0","2","3"],"protocol":"ldap","source":"10.10.22.156"}`

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 4249 / TCP stream 187, frame 4251 / TCP stream 187, frame 4253 / TCP stream 187, frame 4255 / TCP stream 187, frame 4257 / TCP stream 187.

Metrics: `{"destination":"10.10.22.22","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"10.10.22.156"}`

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 127 / TCP stream 3, frame 131 / TCP stream 3, frame 134 / TCP stream 3, frame 145 / TCP stream 3, frame 147 / TCP stream 3.

Metrics: `{"destination":"10.10.22.22","event\_count":49,"operation\_numbers":["0","1","12","30"],"protocol":"drsuapi","source":"10.10.22.157"}`

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 27 / TCP stream 0, frame 91 / TCP stream 5, frame 120 / TCP stream 5, frame 129 / TCP stream 5, frame 133 / TCP stream 5.

Metrics: `{"destination":"10.10.22.22","event\_count":92,"operation\_numbers":["","0","2","3"],"protocol":"ldap","source":"10.10.22.157"}`

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 3468 / TCP stream 157, frame 3470 / TCP stream 157, frame 3472 / TCP stream 157, frame 3474 / TCP stream 157, frame 3476 / TCP stream 157.

Metrics: `{"destination":"10.10.22.22","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"10.10.22.157"}`

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 1951 / TCP stream 93, frame 1959 / TCP stream 93, frame 1963 / TCP stream 93, frame 1964 / TCP stream 86, frame 1968 / TCP stream 86.

Metrics: `{"destination":"10.10.22.22","event\_count":53,"operation\_numbers":["0","1","12","13","30"],"protocol":"drsuapi","source":"10.10.22.158"}`

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 1696 / TCP stream 79, frame 1776 / TCP stream 84, frame 1907 / TCP stream 79, frame 1938 / TCP stream 84, frame 1960 / TCP stream 84.

Metrics: `{"destination":"10.10.22.22","event\_count":88,"operation\_numbers":["","0","2","3"],"protocol":"ldap","source":"10.10.22.158"}`

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 2699 / TCP stream 126, frame 2701 / TCP stream 126, frame 2703 / TCP stream 126, frame 2705 / TCP stream 126, frame 2708 / TCP stream 126.

Metrics: `{"destination":"10.10.22.22","event\_count":43,"operation\_numbers":["1","16","17","18","19","20","25","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"10.10.22.158"}`

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 1000 / TCP stream 46, frame 1002 / TCP stream 46, frame 1004 / TCP stream 46, frame 1014 / TCP stream 46, frame 1016 / TCP stream 46.

Metrics: `{"destination":"10.10.22.156","event\_count":59,"operation\_numbers":["0","1","12","13","30"],"protocol":"drsuapi","source":"10.10.22.22"}`

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 806 / TCP stream 37, frame 968 / TCP stream 37, frame 10

64 / TCP stream 55, frame 1071 / TCP stream 55, frame 1073 / TCP stream 55.

Metrics: `{"destination":"10.10.22.156","event\_count":82,"operation\_numbers":["","1","4,19,19,5","4,5","5"],"protocol":"ldap","source":"10.10.22.22"}`

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 4250 / TCP stream 187, frame 4252 / TCP stream 187, frame 4254 / TCP stream 187, frame 4256 / TCP stream 187, frame 4258 / TCP stream 187.

Metrics: `{"destination":"10.10.22.156","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"10.10.22.22"}`

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 128 / TCP stream 3, frame 132 / TCP stream 3, frame 135 / TCP stream 3, frame 146 / TCP stream 3, frame 150 / TCP stream 3.

Metrics: `{"destination":"10.10.22.157","event\_count":49,"operation\_numbers":["0","1","12","30"],"protocol":"drsuapi","source":"10.10.22.22"}`

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 29 / TCP stream 0, frame 93 / TCP stream 5, frame 124 / TCP stream 5, frame 130 / TCP stream 5, frame 136 / TCP stream 5.

Metrics: `{"destination":"10.10.22.157","event\_count":74,"operation\_numbers":["","1","4,19,19,5","4,5","5"],"protocol":"ldap","source":"10.10.22.22"}`

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 3469 / TCP stream 157, frame 3471 / TCP stream 157, frame 3473 / TCP stream 157, frame 3475 / TCP stream 157, frame 3477 / TCP stream 157.

Metrics: `{"destination":"10.10.22.157","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"10.10.22.22"}`

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 1954 / TCP stream 93, frame 1961 / TCP stream 93, frame 1965 / TCP stream 93, frame 1966 / TCP stream 86, frame 1972 / TCP stream 86.

Metrics: `{"destination":"10.10.22.158","event\_count":53,"operation\_numbers":["0","1","12","13","30"],"protocol":"drsuapi","source":"10.10.22.22"}`

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 1698 / TCP stream 79, frame 1779 / TCP stream 84, frame

1925 / TCP stream 79, frame 1947 / TCP stream 84, frame 1962 / TCP stream 84.

Metrics: `{"destination":"10.10.22.158","event\_count":71,"operation\_numbers":["","1","4,19,19,19,5","4,5","5"],"protocol":"ldap","source":"10.10.22.22"}`

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 2700 / TCP stream 126, frame 2702 / TCP stream 126, frame 2704 / TCP stream 126, frame 2706 / TCP stream 126, frame 2709 / TCP stream 126.

Metrics: `{"destination":"10.10.22.158","event\_count":43,"operation\_numbers":["1","16","17","18","19","20","25","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"10.10.22.22"}`

MEDIUM \u2014 Sustained external TCP conversation outside decoded application coverage

The flow exchanges traffic with a public endpoint but has no HTTP/TLS/identity event in this profile. Inspect the stream for a custom protocol or a missing handshake. This is a coverage/investigation lead, not a malware verdict.

Rule: `unclassified-external-tcp@pcap-rules-v3`; confidence: 0.7; evidence: frame 5644 / TCP stream 232.

Metrics: `{"destination":"37.0.10.22","destination\_port":1187,"duration\_seconds":336.595,"packets":514,"source":"10.10.22.157","wire\_bytes":376928}`

MEDIUM \u2014 Sustained external TCP conversation outside decoded application coverage

The flow exchanges traffic with a public endpoint but has no HTTP/TLS/identity event in this profile. Inspect the stream for a custom protocol or a missing handshake. This is a coverage/investigation lead, not a malware verdict.

Rule: `unclassified-external-tcp@pcap-rules-v3`; confidence: 0.7; evidence: frame 17795 / TCP stream 391.

Metrics: `{"destination":"37.0.10.22","destination\_port":1187,"duration\_seconds":171.549,"packets":72,"source":"10.10.22.157","wire\_bytes":4376}`

MEDIUM \u2014 Sustained external TCP conversation outside decoded application coverage

The flow exchanges traffic with a public endpoint but has no HTTP/TLS/identity event in this profile. Inspect the stream for a custom protocol or a missing handshake. This is a coverage/investigation lead, not a malware verdict.

Rule: `unclassified-external-tcp@pcap-rules-v3`; confidence: 0.7; evidence: frame 24560 / TCP stream 691.

Metrics: `{"destination":"37.0.10.22","destination\_port":1187,"duration\_seconds":330.753,"packets":134,"source":"10.10.22.157","wire\_bytes":8096}`

MEDIUM \u2014 Sustained external TCP conversation outside decoded application coverage

The flow exchanges traffic with a public endpoint but has no HTTP/TLS/identity event in this profile. Inspect the stream for a custom protocol or a missing handshake. This is a coverage/investigation lead, not a malware verdict.

Rule: `unclassified-external-tcp@pcap-rules-v3`; confidence: 0.7; evidence: frame 42858 / TCP stream 810.

Metrics: `{"destination":"23.111.114.52","destination\_port":65400,"duration\_seconds":3322.704,"packets":9622,"source":"10.10.22.156","wire\_bytes":1586196}`

MEDIUM \u2014 Sustained external TCP conversation outside decoded application coverage

The flow exchanges traffic with a public endpoint but has no HTTP/TLS/identity event in this profile. Inspect the stream for a custom protocol or a missing handshake. This is a coverage/investigation lead, not a malware verdict.

Rule: `unclassified-external-tcp@pcap-rules-v3`; confidence: 0.7; evidence: frame 51877 / TCP stream 968.

Metrics: `{"destination":"37.0.10.22","destination\_port":1187,"duration\_seconds":334.618,"packets":136,"source":"10.10.22.157","wire\_bytes":8216}`

MEDIUM \u2014 Sustained external TCP conversation outside decoded application coverage

The flow exchanges traffic with a public endpoint but has no HTTP/TLS/identity event in this profile. Inspect the stream for a custom protocol or a missing handshake. This is a coverage/investigation lead, not a malware verdict.

Rule: `unclassified-external-tcp@pcap-rules-v3`; confidence: 0.7; evidence: frame 61387 / TCP stream 1254.

Metrics: `{\"destination\":\"37.0.10.22\",\"destination\_port\":1187,\"duration\_seconds\":330.634,\"packets\":134,\"source\":\"10.10.22.157\",\"wire\_bytes\":8096}`

MEDIUM \u2014 Sustained external TCP conversation outside decoded application coverage

The flow exchanges traffic with a public endpoint but has no HTTP/TLS/identity event in this profile. Inspect the stream for a custom protocol or a missing handshake. This is a coverage/investigation lead, not a malware verdict.

Rule: `unclassified-external-tcp@pcap-rules-v3`; confidence: 0.7; evidence: frame 67512 / TCP stream 1346.

Metrics: `{\"destination\":\"45.153.241.142\",\"destination\_port\":443,\"duration\_seconds\":699.347,\"packets\":52,\"source\":\"10.10.22.156\",\"wire\_bytes\":3186}`

MEDIUM \u2014 Sustained external TCP conversation outside decoded application coverage

The flow exchanges traffic with a public endpoint but has no HTTP/TLS/identity event in this profile. Inspect the stream for a custom protocol or a missing handshake. This is a coverage/investigation lead, not a malware verdict.

Rule: `unclassified-external-tcp@pcap-rules-v3`; confidence: 0.7; evidence: frame 67513 / TCP stream 1347.

Metrics: `{\"destination\":\"45.153.241.142\",\"destination\_port\":443,\"duration\_seconds\":699.318,\"packets\":54,\"source\":\"10.10.22.156\",\"wire\_bytes\":3306}`

MEDIUM \u2014 Sustained external TCP conversation outside decoded application coverage

The flow exchanges traffic with a public endpoint but has no HTTP/TLS/identity event in this profile. Inspect the stream for a custom protocol or a missing handshake. This is a coverage/investigation lead, not a malware verdict.

Rule: `unclassified-external-tcp@pcap-rules-v3`; confidence: 0.7; evidence: frame 69549 / TCP stream 1450.

Metrics: `{\"destination\":\"37.0.10.22\",\"destination\_port\":1187,\"duration\_seconds\":331.166,\"packets\":132,\"source\":\"10.10.22.157\",\"wire\_bytes\":7976}`

MEDIUM \u2014 Sustained external TCP conversation outside decoded application coverage

The flow exchanges traffic with a public endpoint but has no HTTP/TLS/identity event in this profile. Inspect the stream for a custom protocol or a missing handshake. This is a coverage/investigation lead, not a malware verdict.

Rule: `unclassified-external-tcp@pcap-rules-v3`; confidence: 0.7; evidence: frame 74529 / TCP stream 1485.

Metrics: `{\"destination\":\"45.153.241.142\",\"destination\_port\":443,\"duration\_seconds\":30.11,\"packets\":19,\"source\":\"10.10.22.156\",\"wire\_bytes\":1120}`

MEDIUM \u2014 Sustained external TCP conversation outside decoded application coverage

The flow exchanges traffic with a public endpoint but has no HTTP/TLS/identity event in this profile. Inspect the stream for a custom protocol or a missing handshake. This is a coverage/investigation lead, not a malware verdict.

Rule: `unclassified-external-tcp@pcap-rules-v3`; confidence: 0.7; evidence: frame 76852 / TCP stream 1559.

Metrics: `{\"destination\":\"37.0.10.22\",\"destination\_port\":1187,\"duration\_seconds\":333.255,\"packets\":132,\"source\":\"10.10.22.157\",\"wire\_bytes\":7976}`

MEDIUM \u2014 Sustained external TCP conversation outside decoded application coverage

The flow exchanges traffic with a public endpoint but has no HTTP/TLS/identity event in this profile. Inspect the stream for a custom protocol or a missing handshake. This is a coverage/investigation lead, not a malware verdict.

Rule: `unclassified-external-tcp@pcap-rules-v3`; confidence: 0.7; evidence: frame 81050 / TCP stream 1607.

Metrics: `{ "destination": "37.0.10.22", "destination\_port": 1187, "duration\_seconds": 331.75, "packets": 134, "source": "10.10.22.157", "wire\_bytes": 8096 }`

MEDIUM \u2014 Sustained external TCP conversation outside decoded application coverage

The flow exchanges traffic with a public endpoint but has no HTTP/TLS/identity event in this profile. Inspect the stream for a custom protocol or a missing handshake. This is a coverage/investigation lead, not a malware verdict.

Rule: `unclassified-external-tcp@pcap-rules-v3`; confidence: 0.7; evidence: frame 83774 / TCP stream 1645.

Metrics: `{ "destination": "37.0.10.22", "destination\_port": 1187, "duration\_seconds": 91.986, "packets": 41, "source": "10.10.22.157", "wire\_bytes": 2522 }`

ATT&CK candidates

- No deterministic ATT&CK candidates.

Identities

- account: `agnes.warren`; client IPs: 10.10.22.156; frames: 4153, 4161, 4163, 4175, 4208
- account: `desktop-87wce26\$`; client IPs: 10.10.22.158; frames: 1764, 1791, 1796, 1798, 1809
- account: `desktop-cfa3367\$`; client IPs: 10.10.22.156; frames: 848, 856, 858, 883, 896
- account: `desktop-nz875r4\$`; client IPs: 10.10.22.157; frames: 80, 98, 100, 112, 197
- account: `kevin.henderson`; client IPs: 10.10.22.158; frames: 2596, 2604, 2606, 2618, 2659
- account: `marcus.cobb`; client IPs: 10.10.22.157; frames: 3366, 3374, 3376, 3388, 3431
- domain: `ENEMYWATCH`; client IPs: 10.10.22.156, 10.10.22.157, 10.10.22.158; frames: 2682, 3454, 4233, 56437, 56472
- full-name: `Agnes Warren`; client IPs: 10.10.22.156; frames: 4264
- full-name: `Kevin Henderson`; client IPs: 10.10.22.158; frames: 2715
- full-name: `Marcus Cobb`; client IPs: 10.10.22.157; frames: 3483
- hostname: `DESKTOP-87WCE26`; client IPs: 10.10.22.158; frames: 1667, 1691, 1726, 2106, 2107
- hostname: `DESKTOP-CFA3367`; client IPs: 10.10.22.156; frames: 776, 797, 871, 1183, 1197
- hostname: `DESKTOP-NZ875R4`; client IPs: 10.10.22.157; frames: 1, 42, 333, 343, 545
- netbios-group: `ENEMYWATCH`; client IPs: unbound subject; frames: 43, 342, 546, 625, 626

IOC and artifact candidates

- domain: `112.146.66.173.in-addr.arpa`; roles: dns-query
- domain: `22.22.10.10.in-addr.arpa`; roles: dns-query
- domain: `a-9999.dc.msedge.net`; roles: dns-cname
- domain: `a-ring-fallback.msedge.net`; roles: dns-query, tls-sni
- domain: `a-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `a.nel.cloudflare.com`; roles: dns-query, tls-sni
- domain: `a1449.dscg2.akamai.net`; roles: dns-cname
- domain: `activity-geo.trafficmanager.net`; roles: dns-cname
- domain: `activity.windows.com`; roles: dns-query, tls-sni
- domain: `api.ipify.org`; roles: dns-query, tls-sni
- domain: `api.msn.com`; roles: dns-query, tls-sni
- domain: `aqsouhyw.bazar`; roles: dns-query
- domain: `av.dial-up.net`; roles: dns-query
- domain: `b-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `bing.com`; roles: dns-query, tls-sni
- domain: `bluehail.bazar`; roles: dns-query
- domain: `c-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `calacatta.com`; roles: dns-cname
- domain: `cj.dotomi.com`; roles: dns-query, tls-sni
- domain: `client.wns.windows.com`; roles: dns-query, tls-sni
- domain: `config.edge.skype.com`; roles: dns-query, tls-sni
- domain: `continuum.dds.microsoft.com`; roles: dns-query, tls-sni
- domain: `cs-geo-dds.trafficmanager.net`; roles: dns-cname
- domain: `ctldl.windowsupdate.com`; roles: dns-query, http-host
- domain: `desktop-87wce26.enemywatch.net`; roles: dns-query
- domain: `desktop-cfa3367.enemywatch.net`; roles: dns-query

- domain: `desktop-nz875r4.enemywatch.net`; roles: dns-query
- domain: `dns.msftncsi.com`; roles: dns-query
- domain: `eafddirect.msedge.net`; roles: dns-query
- domain: `edge.activity.windows.com`; roles: dns-query, tls-sni
- domain: `edge.microsoft.com`; roles: dns-query, tls-sni
- domain: `enemywatch-dc.enemywatch.net`; roles: dns-query
- domain: `enemywatch.net`; roles: dns-query
- 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.azurefd.us`; roles: dns-query, tls-sni
- domain: `fp-as.azureedge.net`; roles: dns-query, tls-sni
- domain: `fp-vs-nocache.azureedge.net`; roles: dns-query, tls-sni
- domain: `grtovxn.enemywatch.net`; roles: dns-query
- domain: `grtovxn.localdomain`; roles: dns-query
- domain: `hzm01.mxmail.netease.com`; roles: dns-query, tls-sni
- domain: `imap.gmail.com`; roles: dns-query
- domain: `img-prod-cms-rt-microsoft-com.akamaized.net`; roles: dns-query, tls-sni
- domain: `inbound.att.net`; roles: dns-query
- domain: `k-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `kamuchehddhgfgf.ddns.net`; roles: dns-query
- domain: `l-0005.dc-msedge.net`; roles: dns-cname
- domain: `l-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `login.live.com`; roles: dns-query, tls-sni
- domain: `login.microsoftonline.com`; roles: dns-query, tls-sni
- domain: `mail.abchk.net`; roles: dns-query, tls-sni
- domain: `mail.ajeel.fr`; roles: dns-query, tls-sni
- domain: `mail.akinao-lab.com`; roles: dns-query, tls-sni
- domain: `mail.anberman.es`; roles: dns-query, tls-sni
- domain: `mail.atelierscalin.fr`; roles: dns-query, tls-sni
- domain: `mail.austinjournals.com`; roles: dns-query
- domain: `mail.be-daventure.fr`; roles: dns-query, tls-sni
- domain: `mail.bethnet.co.za`; roles: dns-query, tls-sni
- domain: `mail.brins-d-eveil.fr`; roles: dns-query, tls-sni
- domain: `mail.burgers.cc`; roles: dns-query
- domain: `mail.chokshiandchokshi.in`; roles: dns-query
- domain: `mail.come-paris.fr`; roles: dns-query, tls-sni
- domain: `mail.corteo.fr`; roles: dns-query, tls-sni
- domain: `mail.csnert.fr`; roles: dns-query, tls-sni
- domain: `mail.debtmend.co.za`; roles: dns-query, tls-sni
- domain: `mail.doctor-healthcare.com`; roles: dns-query, tls-sni
- domain: `mail.eolas.fr`; roles: dns-query, tls-sni
- domain: `mail.goldmarkconsultants.com`; roles: dns-query
- domain: `mail.hrctunisia.com`; roles: dns-query, tls-sni
- domain: `mail.ipage.com`; roles: dns-query, tls-sni
- domain: `mail.isoldry.com`; roles: dns-query, tls-sni
- domain: `mail.kalivet.com`; roles: dns-query, tls-sni
- domain: `mail.kbcrawl.net`; roles: dns-query, tls-sni
- domain: `mail.lecmg.fr`; roles: dns-query, tls-sni
- domain: `mail.loosefoot.com`; roles: dns-query
- domain: `mail.ma-communication.com`; roles: dns-query, tls-sni
- domain: `mail.maclen.fr`; roles: dns-query, tls-sni
- domain: `mail.microvistatech.com`; roles: dns-query, tls-sni
- domain: `mail.monquartier.com.br`; roles: dns-query
- domain: `mail.myfairpoint.net`; roles: dns-query
- domain: `mail.nazarioconstruction.com`; roles: dns-query, tls-sni
- domain: `mail.otenet.gr`; roles: dns-query, tls-sni
- domain: `mail.pangia.biz`; roles: dns-query, tls-sni
- domain: `mail.perpetualplaques.com`; roles: dns-query, tls-sni
- domain: `mail.ptolemee.com`; roles: dns-query, tls-sni
- domain: `mail.qualityms.com.mx`; roles: dns-query, tls-sni
- domain: `mail.smtp2go.com`; roles: dns-query
- domain: `mail.songazine.fr`; roles: dns-query, tls-sni
- domain: `mail.tcgasociados.com`; roles: dns-query, tls-sni
- domain: `mail.tecsindia.com`; roles: dns-query

- domain: `mail.tetranergy.com`; roles: dns-query, tls-sni
- domain: `mail.tiretracksusa.com`; roles: dns-query
- domain: `mail.verificalitas.es`; roles: dns-query, tls-sni
- domain: `mail.verificalitasoca.es`; roles: dns-query, tls-sni
- domain: `mail.xenium-partners.fr`; roles: dns-query, tls-sni
- domain: `mail.yourwebsitesmail.com`; roles: dns-query, tls-sni
- domain: `mail04.l4email.com`; roles: dns-query, tls-sni
- domain: `microsoft.com`; roles: dns-query, tls-sni
- domain: `moiazureorigin.clo.footprintdns.com`; roles: dns-query
- domain: `mta-01.webnode.com`; roles: dns-query, tls-sni
- domain: `mta.21cn.com`; roles: dns-query, tls-sni
- domain: `mx.celleno.it`; roles: dns-query
- domain: `mx02.colt-engine.it`; roles: dns-query
- domain: `mx1.mail.139.com`; roles: dns-query, tls-sni
- domain: `myexternalip.com`; roles: dns-query, tls-sni
- domain: `nexusrules.officeapps.live.com`; roles: dns-query, tls-sni
- domain: `ns0.ovh.net`; roles: dns-cname
- domain: `odc.officeapps.live.com`; roles: dns-query, tls-sni
- domain: `oftheearth.ca`; roles: dns-cname
- domain: `outlook.office365.com`; roles: dns-query, tls-sni
- domain: `pingosip.top`; roles: dns-query, tls-sni
- domain: `prod.nexusrules.live.com.akadns.net`; roles: dns-cname
- domain: `pti.store.microsoft.com`; roles: dns-query, tls-sni
- domain: `reddew28c.bazar`; roles: dns-query
- domain: `redinnovations.co.uk`; roles: dns-query, tls-sni
- domain: `rum18.perf.linkedin.com`; roles: dns-query, tls-sni
- domain: `self.events.data.microsoft.com`; 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: `slickdeals.net`; roles: dns-query, tls-sni
- domain: `smtp-com.netzero.net`; roles: dns-cname
- domain: `smtp-relay.gmail.com`; roles: dns-query
- domain: `smtp.forpsi.com`; roles: dns-query, tls-sni
- domain: `smtp.juno.com`; roles: dns-query
- domain: `smtp.medicinafutura.it`; roles: dns-query, tls-sni
- domain: `smtp.netzero.com`; roles: dns-query
- domain: `smtp.outlook.com`; roles: dns-query, tls-sni
- domain: `smtp.sina.com.cn`; roles: dns-query, tls-sni
- domain: `smtp.suddenlink.net`; roles: dns-query, tls-sni
- domain: `smtp.ulpianocarrasco.com`; roles: dns-query, tls-sni
- domain: `smtp.unisanraffaele.gov.it`; roles: dns-query, tls-sni
- domain: `smtp.vox.co.za`; roles: dns-query
- domain: `smtpa.forpsi.com`; roles: dns-cname
- domain: `sobolpand.top`; roles: dns-query, http-host
- domain: `spo-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `ssl0.ovh.net`; roles: dns-cname
- domain: `storeedgefd.dsx.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `t-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `tackleadvisors.com`; roles: dns-query, tls-sni
- domain: `teams-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `track.cj.akadns.net`; roles: dns-cname
- domain: `ultimatecuisinecatering.com`; roles: dns-query, tls-sni
- domain: `umwatson.events.data.microsoft.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: `vchbbq.com`; roles: dns-query, tls-sni
- domain: `vmail.dial-up.net`; roles: dns-cname
- domain: `w00d8b4e.kasserver.com`; roles: dns-query, tls-sni
- domain: `whitestorm9p.bazar`; roles: dns-query
- domain: `wns.notify.trafficmanager.net`; roles: dns-cname
- domain: `wpad.enemywatch.net`; roles: dns-query
- domain: `wpad.localdomain`; roles: dns-query
- domain: `www.backmarket.com`; roles: dns-query, tls-sni
- domain: `www.bing.com`; roles: dns-query, tls-sni
- domain: `www.calacatta.com`; roles: dns-query, tls-sni

- domain: `www.dellrefurbished.com`; roles: dns-query, tls-sni
- domain: `www.emjcd.com`; roles: dns-query, tls-sni
- domain: `www.kqzyfj.com`; roles: dns-query, http-host
- domain: `www.microsoft.com`; roles: dns-query, tls-sni
- domain: `www.offtheearth.ca`; roles: dns-query, tls-sni
- domain: `www.openssl.org`; roles: dns-query, tls-sni
- domain: `x1.c.lencr.org`; roles: dns-query, http-host
- domain: `yeahmx01.mxmail.netease.com`; roles: dns-query, tls-sni
- domain: `znkbmknmqyvbxi.enemywatch.net`; roles: dns-query
- domain: `znkbmknmqyvbxi.localdomain`; roles: dns-query
- domain: `zuczbdyvfzio.enemywatch.net`; roles: dns-query
- domain: `zuczbdyvfzio.localdomain`; roles: dns-query
- ipv4: `0.0.0.0`; roles: network-endpoint
- ipv4: `10.10.22.1`; roles: network-endpoint
- ipv4: `10.10.22.156`; roles: dns-answer, network-endpoint
- ipv4: `10.10.22.157`; roles: dns-answer, network-endpoint
- ipv4: `10.10.22.158`; roles: dns-answer, network-endpoint
- ipv4: `10.10.22.22`; roles: dns-answer, network-endpoint
- ipv4: `10.10.22.255`; roles: network-endpoint
- ipv4: `103.129.255.250`; roles: dns-answer, network-endpoint
- ipv4: `103.129.255.251`; roles: dns-answer
- ipv4: `103.143.8.71`; roles: network-endpoint
- ipv4: `104.16.10.88`; roles: dns-answer, network-endpoint
- ipv4: `104.17.201.57`; roles: dns-answer
- ipv4: `104.208.16.88`; roles: dns-answer, network-endpoint
- ipv4: `104.208.16.94`; roles: dns-answer, network-endpoint
- ipv4: `104.21.32.95`; roles: dns-answer, network-endpoint
- ipv4: `104.21.65.22`; roles: dns-answer
- ipv4: `104.215.148.63`; roles: dns-answer, network-endpoint
- ipv4: `104.46.162.226`; roles: dns-answer, network-endpoint
- ipv4: `104.94.77.31`; roles: dns-answer, network-endpoint
- ipv4: `107.161.180.34`; roles: dns-answer, network-endpoint
- ipv4: `108.168.133.76`; roles: dns-answer, network-endpoint
- ipv4: `111.223.52.28`; roles: dns-answer, network-endpoint
- ipv4: `115.112.78.166`; roles: dns-answer, network-endpoint
- ipv4: `122.179.158.212`; roles: network-endpoint
- ipv4: `123.126.45.161`; roles: dns-answer, network-endpoint
- ipv4: `123.58.177.213`; roles: dns-answer, network-endpoint
- ipv4: `123.58.177.214`; roles: dns-answer
- ipv4: `123.58.177.220`; roles: dns-answer
- ipv4: `129.246.14.238`; roles: dns-answer
- 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: `13.107.4.254`; roles: dns-answer, network-endpoint
- ipv4: `13.107.4.50`; roles: dns-answer
- ipv4: `13.107.42.16`; roles: dns-answer, network-endpoint
- ipv4: `13.107.42.254`; roles: dns-answer, network-endpoint
- ipv4: `13.107.43.14`; roles: dns-answer, network-endpoint
- ipv4: `13.107.6.254`; roles: dns-answer, network-endpoint
- ipv4: `13.64.180.106`; roles: dns-answer, network-endpoint
- ipv4: `13.69.239.72`; roles: dns-answer, network-endpoint
- ipv4: `13.77.161.179`; roles: dns-answer
- ipv4: `13.86.61.82`; roles: dns-answer, network-endpoint
- ipv4: `13.89.178.27`; roles: dns-answer, network-endpoint
- ipv4: `13.89.179.10`; roles: dns-answer, network-endpoint
- ipv4: `13.89.179.9`; roles: dns-answer, network-endpoint
- ipv4: `130.61.64.122`; roles: network-endpoint
- ipv4: `131.107.255.255`; roles: dns-answer
- ipv4: `131.253.33.254`; roles: dns-answer, network-endpoint
- ipv4: `140.82.49.12`; roles: network-endpoint
- ipv4: `142.250.114.108`; roles: dns-answer
- ipv4: `142.250.114.109`; roles: dns-answer, network-endpoint
- ipv4: `142.250.114.28`; roles: dns-answer, network-endpoint

- ipv4: `159.127.40.144`; roles: dns-answer, network-endpoint
- ipv4: `162.210.220.137`; roles: network-endpoint
- ipv4: `167.248.117.81`; roles: network-endpoint
- ipv4: `168.196.133.84`; roles: dns-answer, network-endpoint
- ipv4: `172.67.139.101`; roles: dns-answer, network-endpoint
- ipv4: `172.67.150.172`; roles: dns-answer
- ipv4: `173.223.109.212`; roles: dns-answer, network-endpoint
- ipv4: `173.249.53.15`; roles: dns-answer, network-endpoint
- ipv4: `173.255.233.87`; roles: dns-answer
- ipv4: `178.23.190.8`; roles: http-host, network-endpoint
- ipv4: `180.149.244.81`; roles: dns-answer, network-endpoint
- ipv4: `183.61.185.83`; roles: dns-answer, network-endpoint
- ipv4: `187.250.109.250`; roles: network-endpoint
- ipv4: `189.210.115.207`; roles: network-endpoint
- ipv4: `190.117.91.214`; roles: network-endpoint
- ipv4: `190.14.37.244`; roles: http-host, network-endpoint
- ipv4: `192.185.57.27`; roles: dns-answer, network-endpoint
- ipv4: `193.70.18.144`; roles: dns-answer, network-endpoint
- ipv4: `194.15.112.173`; roles: network-endpoint
- ipv4: `194.36.191.35`; roles: http-host, network-endpoint
- ipv4: `197.221.10.57`; roles: dns-answer, network-endpoint
- ipv4: `197.242.67.121`; roles: dns-answer, network-endpoint
- ipv4: `197.97.195.226`; roles: dns-answer, network-endpoint
- ipv4: `198.136.61.225`; roles: dns-answer, network-endpoint
- ipv4: `198.50.182.64`; roles: dns-answer, network-endpoint
- ipv4: `2.222.167.138`; roles: network-endpoint
- ipv4: `20.140.56.70`; roles: dns-answer, network-endpoint
- ipv4: `20.189.173.12`; roles: dns-answer, network-endpoint
- ipv4: `20.189.173.7`; roles: dns-answer, network-endpoint
- ipv4: `20.190.157.11`; roles: dns-answer, network-endpoint
- ipv4: `20.190.4.251`; roles: dns-answer, network-endpoint
- ipv4: `20.42.4.116`; roles: dns-answer
- ipv4: `20.44.10.123`; roles: dns-answer, network-endpoint
- ipv4: `20.50.80.210`; roles: dns-answer, network-endpoint
- ipv4: `20.69.137.228`; roles: dns-answer, network-endpoint
- ipv4: `20.83.81.162`; roles: dns-answer, network-endpoint
- ipv4: `201.111.144.72`; roles: network-endpoint
- ipv4: `201.137.10.225`; roles: network-endpoint
- ipv4: `204.79.197.200`; roles: dns-answer, network-endpoint
- ipv4: `204.79.197.203`; roles: dns-answer, network-endpoint
- ipv4: `204.79.197.219`; roles: dns-answer, network-endpoint
- ipv4: `204.79.197.254`; roles: dns-answer, network-endpoint
- ipv4: `207.246.112.221`; roles: network-endpoint
- ipv4: `208.180.40.68`; roles: dns-answer, network-endpoint
- ipv4: `208.68.106.6`; roles: dns-answer, network-endpoint
- ipv4: `209.203.34.199`; roles: dns-answer, network-endpoint
- ipv4: `209.210.95.228`; roles: network-endpoint
- ipv4: `217.11.242.15`; roles: dns-answer, network-endpoint
- ipv4: `217.11.242.6`; roles: dns-answer
- ipv4: `217.11.242.81`; roles: dns-answer
- ipv4: `217.116.0.228`; roles: dns-answer, network-endpoint
- ipv4: `221.176.66.188`; roles: dns-answer, network-endpoint
- ipv4: `223.29.248.111`; 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: `23.111.114.52`; roles: network-endpoint
- ipv4: `23.21.76.7`; roles: dns-answer, network-endpoint
- ipv4: `23.222.241.43`; roles: dns-answer, network-endpoint
- ipv4: `23.222.241.55`; roles: dns-answer
- ipv4: `23.23.138.107`; roles: dns-answer
- ipv4: `23.23.229.175`; roles: dns-answer
- ipv4: `23.47.169.181`; roles: dns-answer, network-endpoint
- ipv4: `23.47.50.172`; roles: dns-answer
- ipv4: `23.47.50.180`; roles: dns-answer, network-endpoint

- ipv4: `23.47.52.13`; roles: dns-answer, network-endpoint
- ipv4: `23.47.52.19`; roles: dns-answer
- ipv4: `239.255.255.250`; roles: http-host, network-endpoint
- ipv4: `24.231.209.2`; roles: network-endpoint
- ipv4: `255.255.255.255`; roles: dns-answer, network-endpoint
- ipv4: `26.85.198.164`; roles: dns-answer
- ipv4: `31.193.50.122`; roles: dns-answer, network-endpoint
- ipv4: `31.193.50.2`; roles: dns-answer
- ipv4: `34.117.59.81`; roles: dns-answer, network-endpoint
- ipv4: `34.120.119.232`; roles: dns-answer, network-endpoint
- ipv4: `34.149.19.242`; roles: network-endpoint
- ipv4: `34.193.71.224`; roles: dns-answer, network-endpoint
- ipv4: `35.190.80.1`; roles: dns-answer, network-endpoint
- ipv4: `37.0.10.22`; roles: dns-answer, network-endpoint
- ipv4: `37.208.181.198`; roles: network-endpoint
- ipv4: `37.252.0.102`; roles: network-endpoint
- ipv4: `39.40.37.70`; roles: network-endpoint
- ipv4: `40.112.72.205`; roles: dns-answer
- ipv4: `40.113.200.201`; roles: dns-answer
- ipv4: `40.126.28.11`; roles: dns-answer, network-endpoint
- ipv4: `40.126.28.12`; roles: dns-answer, network-endpoint
- ipv4: `40.126.28.13`; roles: dns-answer
- ipv4: `40.126.28.14`; roles: dns-answer
- ipv4: `40.126.28.18`; roles: dns-answer
- ipv4: `40.126.28.19`; roles: dns-answer
- ipv4: `40.126.28.20`; roles: dns-answer, network-endpoint
- ipv4: `40.126.28.21`; roles: dns-answer
- ipv4: `40.126.28.22`; roles: dns-answer, network-endpoint
- ipv4: `40.126.28.23`; roles: dns-answer, network-endpoint
- ipv4: `40.126.29.10`; roles: dns-answer
- ipv4: `40.126.29.11`; roles: dns-answer, network-endpoint
- ipv4: `40.126.29.12`; roles: dns-answer, network-endpoint
- ipv4: `40.126.29.13`; roles: dns-answer
- ipv4: `40.126.29.14`; roles: dns-answer
- ipv4: `40.126.29.15`; roles: dns-answer, network-endpoint
- ipv4: `40.126.29.5`; roles: dns-answer, network-endpoint
- ipv4: `40.126.29.7`; roles: dns-answer
- ipv4: `40.126.29.8`; roles: dns-answer, network-endpoint
- ipv4: `40.126.29.9`; roles: dns-answer
- ipv4: `40.126.7.32`; roles: dns-answer
- ipv4: `40.126.7.35`; roles: dns-answer
- ipv4: `40.76.4.15`; roles: dns-answer
- ipv4: `40.90.64.59`; roles: dns-answer, network-endpoint
- ipv4: `40.90.64.61`; roles: dns-answer, network-endpoint
- ipv4: `40.90.64.98`; roles: dns-answer, network-endpoint
- ipv4: `40.97.120.130`; roles: dns-answer
- ipv4: `40.97.120.146`; roles: dns-answer, network-endpoint
- ipv4: `40.97.120.178`; roles: dns-answer
- ipv4: `40.97.120.194`; roles: dns-answer
- ipv4: `40.97.120.210`; roles: dns-answer
- ipv4: `40.97.120.226`; roles: dns-answer, network-endpoint
- ipv4: `40.97.120.242`; roles: dns-answer, network-endpoint
- ipv4: `40.97.120.50`; roles: dns-answer
- ipv4: `40.97.120.66`; roles: dns-answer
- ipv4: `40.97.121.18`; roles: dns-answer, network-endpoint
- ipv4: `40.97.121.2`; roles: dns-answer
- ipv4: `40.97.121.34`; roles: dns-answer
- ipv4: `40.97.199.114`; roles: dns-answer, network-endpoint
- ipv4: `40.97.212.18`; roles: dns-answer
- ipv4: `40.97.212.2`; roles: dns-answer, network-endpoint
- ipv4: `40.97.92.34`; roles: dns-answer
- ipv4: `40.97.96.2`; roles: dns-answer
- ipv4: `41.86.105.101`; roles: dns-answer, network-endpoint
- ipv4: `45.153.241.142`; roles: network-endpoint
- ipv4: `45.33.53.153`; roles: dns-answer

- ipv4: `45.46.53.140`; roles: network-endpoint
- ipv4: `45.79.114.202`; roles: dns-answer
- ipv4: `45.79.170.99`; roles: dns-answer
- ipv4: `45.79.71.155`; roles: dns-answer
- ipv4: `47.151.181.188`; roles: network-endpoint
- ipv4: `47.22.148.6`; roles: network-endpoint
- ipv4: `47.40.196.233`; roles: network-endpoint
- ipv4: `50.16.216.118`; roles: dns-answer
- ipv4: `50.16.235.219`; roles: dns-answer
- ipv4: `50.16.239.65`; roles: dns-answer
- ipv4: `50.17.218.95`; roles: dns-answer, network-endpoint
- ipv4: `50.17.226.156`; roles: dns-answer
- ipv4: `50.19.104.221`; roles: dns-answer
- ipv4: `50.19.250.64`; roles: dns-answer
- ipv4: `50.19.81.52`; roles: dns-answer
- ipv4: `50.19.92.180`; roles: dns-answer
- ipv4: `50.194.160.233`; roles: network-endpoint
- ipv4: `50.77.156.245`; roles: dns-answer, network-endpoint
- ipv4: `51.132.193.105`; roles: dns-answer, network-endpoint
- ipv4: `51.158.108.203`; roles: network-endpoint
- ipv4: `52.109.2.1`; roles: dns-answer, network-endpoint
- ipv4: `52.109.76.31`; roles: dns-answer, network-endpoint
- ipv4: `52.109.76.32`; roles: dns-answer, network-endpoint
- ipv4: `52.109.8.20`; roles: dns-answer, network-endpoint
- ipv4: `52.113.196.254`; roles: dns-answer, network-endpoint
- ipv4: `52.152.108.96`; roles: dns-answer, network-endpoint
- ipv4: `52.178.17.3`; roles: dns-answer, network-endpoint
- ipv4: `52.182.143.210`; roles: dns-answer, network-endpoint
- ipv4: `52.183.220.149`; roles: dns-answer, network-endpoint
- ipv4: `52.185.211.133`; roles: dns-answer, network-endpoint
- ipv4: `52.232.226.150`; roles: dns-answer, network-endpoint
- ipv4: `52.242.97.97`; roles: dns-answer, network-endpoint
- ipv4: `52.96.10.242`; roles: dns-answer, network-endpoint
- ipv4: `52.96.103.18`; roles: dns-answer, network-endpoint
- ipv4: `52.96.103.2`; roles: dns-answer, network-endpoint
- ipv4: `52.96.103.34`; roles: dns-answer, network-endpoint
- ipv4: `52.96.121.114`; roles: dns-answer, network-endpoint
- ipv4: `52.96.121.130`; roles: dns-answer
- ipv4: `52.96.121.146`; roles: dns-answer
- ipv4: `52.96.121.162`; roles: dns-answer, network-endpoint
- ipv4: `52.96.121.178`; roles: dns-answer
- ipv4: `52.96.121.194`; roles: dns-answer, network-endpoint
- ipv4: `52.96.121.210`; roles: dns-answer, network-endpoint
- ipv4: `52.96.121.242`; roles: dns-answer
- ipv4: `52.96.121.98`; roles: dns-answer, network-endpoint
- ipv4: `52.96.122.226`; roles: dns-answer, network-endpoint
- ipv4: `52.96.122.242`; roles: dns-answer, network-endpoint
- ipv4: `52.96.122.98`; roles: dns-answer
- ipv4: `52.96.16.162`; roles: dns-answer, network-endpoint
- ipv4: `52.96.191.114`; roles: dns-answer
- ipv4: `52.96.191.98`; roles: dns-answer, network-endpoint
- ipv4: `52.96.22.178`; roles: dns-answer, network-endpoint
- ipv4: `52.96.22.2`; roles: dns-answer
- ipv4: `52.96.55.242`; roles: dns-answer, network-endpoint
- ipv4: `52.96.57.18`; roles: dns-answer, network-endpoint
- ipv4: `52.96.57.2`; roles: dns-answer, network-endpoint
- ipv4: `52.96.57.34`; roles: dns-answer
- ipv4: `52.96.57.50`; roles: dns-answer
- ipv4: `52.96.57.66`; roles: dns-answer
- ipv4: `52.96.57.82`; roles: dns-answer, network-endpoint
- ipv4: `52.96.57.98`; roles: dns-answer
- ipv4: `52.96.8.130`; roles: dns-answer
- ipv4: `52.96.90.18`; roles: dns-answer, network-endpoint
- ipv4: `52.96.91.66`; roles: dns-answer, network-endpoint
- ipv4: `54.243.250.193`; roles: dns-answer, network-endpoint

- ipv4: `54.243.253.71`; roles: dns-answer
- ipv4: `54.243.29.214`; roles: dns-answer, network-endpoint
- ipv4: `54.243.41.12`; roles: dns-answer
- ipv4: `54.243.51.135`; roles: dns-answer
- ipv4: `60.241.142.83`; roles: dns-answer
- ipv4: `62.103.147.201`; roles: dns-answer, network-endpoint
- ipv4: `62.149.128.200`; roles: dns-answer
- ipv4: `62.149.128.201`; roles: dns-answer
- ipv4: `62.149.128.202`; roles: dns-answer
- ipv4: `62.149.128.203`; roles: dns-answer, network-endpoint
- ipv4: `64.136.44.45`; roles: dns-answer
- ipv4: `64.136.44.50`; roles: dns-answer
- ipv4: `64.136.52.45`; roles: dns-answer, network-endpoint
- ipv4: `64.136.52.50`; roles: dns-answer, network-endpoint
- ipv4: `64.29.151.102`; roles: dns-answer, network-endpoint
- ipv4: `64.87.23.16`; roles: dns-answer, network-endpoint
- ipv4: `64.98.36.176`; roles: dns-answer, network-endpoint
- ipv4: `65.111.191.196`; roles: dns-answer, network-endpoint
- ipv4: `65.254.248.195`; roles: dns-answer, network-endpoint
- ipv4: `66.163.170.35`; roles: dns-answer
- ipv4: `66.218.88.149`; roles: dns-answer, network-endpoint
- ipv4: `66.218.88.150`; roles: dns-answer
- ipv4: `66.218.88.152`; roles: dns-answer
- ipv4: `66.218.88.154`; roles: dns-answer
- ipv4: `66.218.88.155`; roles: dns-answer
- ipv4: `66.218.88.157`; roles: dns-answer
- ipv4: `66.218.88.158`; roles: dns-answer
- ipv4: `66.228.43.14`; roles: dns-answer, network-endpoint
- ipv4: `66.96.147.96`; roles: dns-answer, network-endpoint
- ipv4: `66.96.162.198`; roles: dns-answer, network-endpoint
- ipv4: `68.186.192.69`; roles: network-endpoint
- ipv4: `68.204.7.158`; roles: network-endpoint
- ipv4: `70.39.150.220`; roles: dns-answer, network-endpoint
- ipv4: `72.21.81.200`; roles: dns-answer, network-endpoint
- ipv4: `72.247.207.22`; roles: dns-answer, network-endpoint
- ipv4: `72.252.201.69`; roles: network-endpoint
- ipv4: `73.230.205.91`; roles: network-endpoint
- ipv4: `73.52.50.32`; roles: network-endpoint
- ipv4: `73.77.87.137`; roles: network-endpoint
- ipv4: `74.202.142.20`; roles: dns-answer, network-endpoint
- ipv4: `8.248.163.254`; roles: dns-answer, network-endpoint
- ipv4: `8.249.123.254`; roles: dns-answer
- ipv4: `8.249.219.254`; roles: dns-answer
- ipv4: `8.249.239.254`; roles: dns-answer
- ipv4: `8.249.245.254`; roles: dns-answer, network-endpoint
- ipv4: `8.253.131.120`; roles: dns-answer
- ipv4: `8.253.156.120`; roles: dns-answer, network-endpoint
- ipv4: `8.253.45.214`; roles: dns-answer
- ipv4: `8.8.8.8`; roles: network-endpoint
- ipv4: `80.6.192.58`; roles: network-endpoint
- ipv4: `81.2.195.204`; roles: dns-answer, network-endpoint
- ipv4: `81.241.252.59`; roles: network-endpoint
- ipv4: `81.31.145.212`; roles: dns-answer
- ipv4: `81.31.145.216`; roles: dns-answer, network-endpoint
- ipv4: `82.98.154.100`; roles: dns-answer, network-endpoint
- ipv4: `83.223.99.191`; roles: dns-answer, network-endpoint
- ipv4: `83.243.251.46`; roles: network-endpoint
- ipv4: `85.13.132.2`; roles: dns-answer, network-endpoint
- ipv4: `86.8.177.143`; roles: network-endpoint
- ipv4: `89.137.52.44`; roles: network-endpoint
- ipv4: `9.241.189.20`; roles: dns-answer
- ipv4: `94.143.155.83`; roles: dns-answer, network-endpoint
- ipv4: `94.200.181.154`; roles: network-endpoint
- ja3: `28a2c9bd18a11de089ef85a160da29e4`; roles: tls-client-fingerprint
- ja3: `29a54baac595d45c6a62225f7cde467b`; roles: tls-client-fingerprint

```

- ja3: `37f463bf4616ecd445d4a1937da06e19`; roles: tls-client-fingerprint
- ja3: `3b5074b1b5d032e5620f69f9f700ff0e`; roles: tls-client-fingerprint
- ja3: `51c64c77e60f3980eea90869b68c58a8`; roles: tls-client-fingerprint
- ja3: `6271f898ce5be7dd52b0fc260d0662b3`; roles: tls-client-fingerprint
- ja3: `89be98bbd4f065fe510fca4893cf8d9b`; roles: tls-client-fingerprint
- ja3: `a0e9f5d64349fb13191bc781f81f42e1`; roles: tls-client-fingerprint
- ja3: `cd08e31494f9531f560d64c695473da9`; roles: tls-client-fingerprint
- ja3: `df669e7ea913f1ac0c0cce9a201a2ec1`; roles: tls-client-fingerprint
- sha256: `11f3d84aad7131fe124155c9edfceb594649e87de1ee03383f470442d6ed69a1`; roles: exported-object
- sha256: `17c18c10640debcd5b5f61f07b12d7327809410c3a90f7cd69f21fb869554ea`; roles: exported-object
- sha256: `95928b331e9942e4709b41ec8b59eb6f9e068f53ef2eeb15009feafd4ff5138d`; roles: exported-object
- sha256: `c8da41ae6e70a1997020d6c903d2627a3ee35383159cd04de53e73ff3f5acd82`; roles: exported-object
- url: `http://178.23.190.8/44491.6090605324.dat`; roles: http-request
- url: `http://190.14.37.244/44491.6090605324.dat`; roles: http-request
- url: `http://194.36.191.35/44491.6090605324.dat`; roles: http-request
- url: `http://239.255.255.250:1900*`; roles: http-request
- url: `http://ctdl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?29290d2fe073e937`; roles: http-request
- url: `http://ctdl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?c6f9855cb9e658e6`; roles: http-request
- url: `http://ctdl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?069916a09ccd9a98`; roles: http-request
- exported object `44491.6090605324(1).dat`; SHA-256 `95928b331e9942e4709b41ec8b59eb6f9e068f53ef2eeb15009feafd4ff5138d`; size 911 360 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 `main.php`; SHA-256 `11f3d84aad7131fe124155c9edfceb594649e87de1ee03383f470442d6ed69a1`; size 337420 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 `index.php`; SHA-256 `c8da41ae6e70a1997020d6c903d2627a3ee35383159cd04de53e73ff3f5acd82`; size 183 bytes
  Static content: `{"content_kind":"script-like-text","features":{"excerpt":"downloadfile","feature":"powershell-download","offset":83},"inspected_bytes":183,"inspection_truncated":false,"interpretation":"Static content only; not proof of execution, intent, or malware family"}`. Not execution proof.
- exported object `click-1225267-10537174-1463076242000%3fsid=552795f4335011ec81850e774cf9d6690INT`; SHA-256 `17c18c10640debcd5b5f61f07b12d7327809410c3a90f7cd69f21fb869554ea`; size 577 bytes

```

Actor similarity leads

- No actor lead was calculated.

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: `5222f776b8c48e86a0c8622f8a6c5757c219009df704244b52c91467fdafc237`; recorded 2026-09-19T12:10:24.874416+00:00; mode: local-only.

Coverage: `{"matched\_observables":0,"no\_exact\_match":512,"observable\_limit":5000,"observables\_checked":512,"observables\_total":512,"prior\_case\_limit\_reached":false,"prior\_cases\_checked":14,"truncated":false}`

```

- Prior analysis `96e0e828-93ae-49d5-8104-9f14cb584c3e` shares 31 observations. This does not establish a common campaign.
- Prior analysis `6e50c68f-5552-400c-9835-15867ddb022d` shares 25 observations. This does not establish a common campaign.
- Prior analysis `43bc93eb-d6db-4400-b983-b0dd404c8ca4` shares 69 observations. This does not establish a common campaign.
- Prior analysis `6df36b51-4b44-4660-b534-2fa89705e807` shares 37 observations. This does not establish a common campaign.
- Prior analysis `29aa3ef8-47c9-4c47-b4cc-1ff3e0708142` shares 27 observations. This does not establish a common campaign.
- Prior analysis `b79032a8-d69e-4ac1-bdd4-542473fa8e3b` shares 30 observations. This does not establish a common campaign.
- Prior analysis `faf041c3-70e0-4a01-8780-10917e5e187c` shares 27 observations. This does not establish a common campaign.
- Prior analysis `08324647-35af-4af2-8d82-4387eec03918` shares 22 observations. This does not establish a common campaign.
- Prior analysis `616a90fa-f15e-4fcb-8d56-7b8e0eff5785` shares 16 observations. This does not establish a common campaign.
- Prior analysis `459e119d-191f-49e8-85ea-c78f9de41826` shares 22 observations. This does not establish a common campaign.
- Prior analysis `7a2cfe72-f48d-4894-8a2d-8889cb3b11b2` shares 43 observations. This does not establish a common campaign.
- Prior analysis `81373b30-6a59-49d1-89b0-bad73ed19eaa` shares 24 observations. This does not establish a common campaign.
- Prior analysis `38851ad7-b3a0-423d-ae89-3b7be4e4b908` shares 34 observations. This does not establish a common campaign.
- Prior analysis `bfccc426-aa9b-4007-8558-a66d37ecb90c` shares 43 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":4, "exported_objects":6, "hashed_bytes":3072260, "hashed_objects":6, "omitted_unique_hashes":0, "returned_unique_hashes":4, "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":4 }`. 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 37/37, identities 14/14, observables 500/512, artifacts 4/4. Full returned inventory is in the JSON result.