

AdversaryGraph

Threat Intelligence Analysis Report

Analysis Metadata

Provider:	deterministic
Model:	tshark-evidence-v3
Domain:	enterprise-attack
Session ID:	df6c55a2-3630-4e95-82d0-0eebb41c3b51
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 5091 packets across 42 IP endpoints and 221 transport flows. Observed 173 DNS events, 57 HTTP requests, 72 TLS ClientHello events, and 6 exported HTTP object(s). Deterministic rules produced 8 finding(s): 0 high, 1 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: 18200 / 18200 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

- gate_pending:source_provenance
- gate_pending:publication_date
- gate_pending:procedure_relevance
- gate_pending:procedure_level_claim
- gate_pending:actor_identification
- claims_unresolved:138
- 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: 2024-09-04-traffic-analysis-exercise.pcap

Capture SHA-256: `8fee06d0b1686faab4364f5b7a741e736ad7e713d5ca9299ff9161a4b4d4862e`

Semantic result SHA-256: `4897ba23edbbda370beb304db04a336b3872d332b86d9834b16bb29e87c6d8b5`

Analyzer manifest SHA-256: `ee952aeb7cdc6958f4ae5178c54c274a1e4f0aec4d42f3bdb95baaff063b3dde`

Executive summary

Decoded 5091 packets across 42 IP endpoints and 221 transport flows. Observed 173 DNS events, 57 HTTP requests, 72 TLS ClientHello events, and 6 exported HTTP object(s). Deterministic rules produced 8 finding(s): 0 high, 1 medium, and 7 low. Findings are evidence-bound candidates and require analyst review; encrypted payload contents remain unavailable.

Capture facts

- Packets: 5091
- Duration: 3576.159984 seconds
- Captured bytes: 2048179
- Endpoints: 42
- Flows: 221

Deterministic findings

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 1668 / TCP stream 48, frame 1672 / TCP stream 48, frame 1697 / TCP stream 48, frame 2347 / TCP stream 56, frame 2985 / TCP stream 63.

Metrics: `{ "declared_body_bytes": 2046, "destination": "79.124.78.197", "host": "79.124.78.197", "port": 80, "request_count": 48, "source": "172.17.0.99", "uri": "/foots.php" }

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 42, frame 111, frame 112, frame 215.

Metrics: `{ "domain": "wpad.bepositive.com", "response_count": 20, "source": "172.17.0.99" }

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 384 / TCP stream 14, frame 386 / TCP stream 14, frame 388 / TCP stream 14, frame 391 / TCP stream 14, frame 1074 / TCP stream 34.

Metrics: `{ "destination": "172.17.0.99", "event_count": 39, "operation_numbers": ["0", "1", "12"], "protocol": "drsuapi", "source": "172.17.0.17" }

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 33 / TCP stream 0, frame 419 / TCP stream 18, frame 431 / TCP stream 18, frame 452 / TCP stream 19, frame 455 / TCP stream 19.

Metrics: `{"destination":"172.17.0.99","event\_count":66,"operation\_numbers":["","1","4,19,19,19,5","4,5","5"],"protocol":"ldap","source":"172.17.0.17"}`

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 410 / TCP stream 13, frame 415 / TCP stream 13, frame 417 / TCP stream 13, frame 420 / TCP stream 13, frame 422 / TCP stream 13.

Metrics: `{"destination":"172.17.0.99","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"172.17.0.17"}`

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 382 / TCP stream 14, frame 385 / TCP stream 14, frame 387 / TCP stream 14, frame 389 / TCP stream 14, frame 1073 / TCP stream 34.

Metrics: `{"destination":"172.17.0.17","event\_count":39,"operation\_numbers":["0","1","12"],"protocol":"druapi","source":"172.17.0.99"}`

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 31 / TCP stream 0, frame 34 / TCP stream 0, frame 412 / TCP stream 18, frame 430 / TCP stream 18, frame 443 / TCP stream 19.

Metrics: `{"destination":"172.17.0.17","event\_count":84,"operation\_numbers":["","0","2","3"],"protocol":"ldap","source":"172.17.0.99"}`

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 409 / TCP stream 13, frame 413 / TCP stream 13, frame 416 / TCP stream 13, frame 418 / TCP stream 13, frame 421 / TCP stream 13.

Metrics: `{"destination":"172.17.0.17","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"172.17.0.99"}`

ATT&CK candidates

- No deterministic ATT&CK candidates.

Identities

- account: `afletcher`; client IPs: 172.17.0.99; frames: 293, 301, 303, 317, 350
- full-name: `Andrew Fletcher`; client IPs: 172.17.0.99; frames: 428
- hostname: `DESKTOP-RNVO9AT`; client IPs: 172.17.0.99; frames: 1, 3, 20, 22, 60
- netbios-group: `BEPOSITIVE`; client IPs: unbound subject; frames: 21, 61, 65, 82, 85

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: `arc.msn.com`; roles: dns-query, tls-sni
- domain: `assets.msn.com`; roles: dns-query, tls-sni
- domain: `bepositive.com`; roles: dns-query

- domain: `blob.mwh03prd02a.store.core.windows.net`; roles: dns-cname
- domain: `client.wns.windows.com`; roles: tls-sni
- domain: `ctdl.windowsupdate.com`; roles: dns-query, http-host
- domain: `desktop-rnvo9at.bepositive.com`; roles: dns-query
- domain: `dns.msftncsi.com`; roles: dns-query
- domain: `download.windowsupdate.com`; roles: dns-query
- domain: `ecs.office.com`; roles: dns-query, tls-sni
- domain: `fd.api.iris.microsoft.com`; roles: dns-query, tls-sni
- domain: `g.live.com`; roles: dns-query, tls-sni
- domain: `img-s-msn-com.akamaized.net`; roles: dns-query, tls-sni
- domain: `inputsuggestions.msdxcdn.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: `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: `pti.store.microsoft.com`; roles: dns-query
- domain: `settings-win.data.microsoft.com`; roles: dns-query, tls-sni
- domain: `srtb.msn.com`; roles: dns-query, tls-sni
- domain: `sso.godaddy.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: `weathermapdata.blob.core.windows.net`; roles: dns-query, tls-sni
- domain: `win-ctl9xbq9y19.bepositive.com`; roles: dns-query
- domain: `windows.msn.com`; roles: dns-query, tls-sni
- domain: `wpad.bepositive.com`; roles: dns-query
- domain: `www.bellantonicioccolato.it`; roles: tls-sni
- 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
- domain: `x1.c.lencr.org`; roles: dns-query, http-host
- ipv4: `0.0.0.0`; roles: network-endpoint
- ipv4: `13.107.246.57`; roles: dns-answer, network-endpoint
- ipv4: `13.70.79.200`; roles: dns-answer, network-endpoint
- ipv4: `13.89.179.9`; roles: dns-answer, network-endpoint
- ipv4: `131.107.255.255`; roles: dns-answer
- ipv4: `172.17.0.17`; roles: dns-answer, network-endpoint
- ipv4: `172.17.0.255`; roles: network-endpoint
- ipv4: `172.17.0.99`; roles: dns-answer, network-endpoint
- ipv4: `184.29.137.96`; roles: dns-answer, network-endpoint
- ipv4: `199.232.210.172`; roles: dns-answer, network-endpoint
- ipv4: `199.232.214.172`; roles: dns-answer, network-endpoint
- ipv4: `20.10.31.115`; roles: network-endpoint
- ipv4: `20.189.173.1`; roles: dns-answer, network-endpoint
- ipv4: `20.189.173.18`; roles: dns-answer, network-endpoint
- ipv4: `20.189.173.26`; roles: dns-answer, network-endpoint
- ipv4: `20.190.135.2`; roles: dns-answer
- ipv4: `20.241.44.114`; roles: dns-answer, network-endpoint
- ipv4: `20.42.73.28`; 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: `204.79.197.203`; roles: dns-answer, 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: `23.195.212.189`; roles: dns-answer, network-endpoint
- ipv4: `23.220.251.149`; roles: dns-answer, network-endpoint
- ipv4: `23.220.251.153`; roles: dns-answer, network-endpoint
- ipv4: `23.220.251.158`; roles: dns-answer, network-endpoint
- ipv4: `23.220.251.160`; roles: dns-answer
- ipv4: `23.220.251.47`; roles: dns-answer, network-endpoint
- ipv4: `23.220.251.48`; roles: dns-answer
- ipv4: `23.221.24.49`; roles: dns-answer
- ipv4: `23.221.24.50`; roles: dns-answer

- ipv4: `23.221.24.51`; roles: dns-answer
- ipv4: `23.221.24.52`; roles: dns-answer
- ipv4: `23.221.24.53`; roles: dns-answer
- ipv4: `23.221.24.55`; roles: dns-answer
- ipv4: `23.221.24.56`; roles: dns-answer
- ipv4: `23.221.24.57`; roles: dns-answer
- ipv4: `23.221.24.58`; roles: dns-answer, network-endpoint
- ipv4: `23.221.24.62`; roles: dns-answer
- ipv4: `23.221.24.63`; roles: dns-answer
- ipv4: `23.221.24.64`; roles: dns-answer
- ipv4: `23.221.24.68`; roles: dns-answer
- ipv4: `23.221.24.69`; roles: dns-answer, network-endpoint
- ipv4: `23.221.24.70`; roles: dns-answer
- ipv4: `23.221.24.73`; roles: dns-answer
- ipv4: `23.40.145.142`; roles: dns-answer, network-endpoint
- ipv4: `23.45.119.134`; roles: dns-answer
- ipv4: `23.45.119.140`; roles: dns-answer
- ipv4: `23.45.119.142`; roles: dns-answer
- ipv4: `23.45.119.143`; roles: dns-answer, network-endpoint
- ipv4: `23.45.119.144`; roles: dns-answer, network-endpoint
- ipv4: `23.45.119.146`; roles: dns-answer
- ipv4: `23.45.119.147`; roles: dns-answer, network-endpoint
- ipv4: `23.45.119.166`; roles: dns-answer
- ipv4: `23.45.119.174`; roles: dns-answer
- ipv4: `255.255.255.255`; roles: network-endpoint
- ipv4: `40.119.249.228`; roles: dns-answer, network-endpoint
- ipv4: `40.126.28.11`; roles: dns-answer
- ipv4: `40.126.28.12`; roles: dns-answer, network-endpoint
- ipv4: `40.126.28.13`; 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
- 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
- ipv4: `40.126.7.32`; roles: dns-answer
- ipv4: `40.126.7.35`; roles: dns-answer
- ipv4: `46.254.34.201`; roles: network-endpoint
- ipv4: `52.109.0.142`; roles: dns-answer, network-endpoint
- ipv4: `52.109.0.91`; roles: dns-answer, network-endpoint
- ipv4: `52.113.194.132`; roles: dns-answer, network-endpoint
- ipv4: `79.124.78.197`; roles: http-host, network-endpoint
- ja3: `091f51a7a1c3a4504a224cc081ce9cee`; roles: tls-client-fingerprint
- ja3: `1a0fcf72de58b80a8499dea99e961714`; roles: tls-client-fingerprint
- ja3: `350c9b4a3f847974933dd25e9f9dc620`; roles: tls-client-fingerprint
- ja3: `3c293bdf2a25c07559b560ba86debc77`; roles: tls-client-fingerprint
- ja3: `3c4eb72b882d4d1442c67ce73f1292a9`; roles: tls-client-fingerprint
- ja3: `4c6de70d03b552090a8d77fcb0e10629`; roles: tls-client-fingerprint
- ja3: `5291cc6eebf72ef2ca72d48a1dd0d72f`; roles: tls-client-fingerprint
- ja3: `5919f6108f098e14c2f37619021ebd4d`; roles: tls-client-fingerprint
- ja3: `65005c9d9ae0f0ebeaf22c210571d482`; roles: tls-client-fingerprint
- ja3: `6a5d235ee78c6aede6a61448b4e9ff1e`; roles: tls-client-fingerprint
- ja3: `81e0f23545c783a55096f99f7c4755d7`; roles: tls-client-fingerprint
- ja3: `a25c14084d58bfea7bb5de112124edb3`; roles: tls-client-fingerprint
- ja3: `a35e0e26a8a46900d0f8297769d1112c`; roles: tls-client-fingerprint
- ja3: `cad306d4b414c5fcf993c03e0d596109`; roles: tls-client-fingerprint
- ja3: `f06a64ec6ecba24167cfe2612badcd91`; roles: tls-client-fingerprint
- sha256: `3f39d5c348e5b79d06e842c114e6cc571583bbf44e4b0ebfda1a01ec05745d43`; roles: exported-object
- sha256: `5e9a7996fe94d7be10595d7133748760bf8348198b71b7a50fd8affaa980ac61`; roles: exported-object
- sha256: `69bf0bc46f51b33377c4f3d92caf876714f6bbbe99e7544487327920873f9820`; roles: exported-object
- sha256: `736f0cb5cc23435dad920dbe447efcf102e61c8691fa8528f5f39f386537f43e`; roles: exported-object
- sha256: `e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855`; roles: exported-object
- sha256: `ed0855c1637e5f93be7d54acb2cb8872683a0e5eb670258abb1ebc41bfbf4591`; roles: exported-object
- url: `http://79.124.78.197/foots.php`; roles: http-request
- url: `http://79.124.78.197/index.php`; roles: http-request

- url: `http://79.124.78.197/index.php?id=&subid=qOUKk7U`; 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?d7a8a57aa5acd39b`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?91717f420e6dda94`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?a5fef2ac8502b132`; roles: http-request
- url: `http://www.msftconnecttest.com/connecttest.txt`; roles: http-request
- url: `http://x1.c.lencr.org/`; 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 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)`; 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)`; roles: http-client
- exported object `index.php`; SHA-256 `ed0855c1637e5f93be7d54acb2cb8872683a0e5eb670258abb1ebc41bfbf4591`; size 105 bytes
- exported object `index.php%3fid=&subid=qOUKk7U`; SHA-256 `736f0cb5cc23435dad920dbe447efcf102e61c8691fa8528f5f39f386537f43e`; size 61 bytes
- exported object `connecttest(1).txt`; SHA-256 `5e9a7996fe94d7be10595d7133748760bf8348198b71b7a50fd8affaa980ac61`; size 22 bytes
- exported object `ProcessMAU.txt`; SHA-256 `69bf0bc46f51b33377c4f3d92caf876714f6bbbe99e7544487327920873f9820`; size 4 bytes
- exported object `index(1).php`; SHA-256 `3f39d5c348e5b79d06e842c114e6cc571583bbf44e4b0ebfda1a01ec05745d43`; size 1 bytes
- exported object `foots(1).php`; SHA-256 `e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855`; size 0 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: `99bf9b0d5c90e5eb36c1f5a055241fc0beb1b677bd448cb59545c1ac1d629049`; recorded 2026-09-19T12:08:45.501397+00:00; mode: local-only.

Coverage: `{ "matched\_observables": 0, "no\_exact\_match": 147, "observable\_limit": 5000, "observables\_checked": 147, "observables\_total": 147, "prior\_case\_limit\_reached": false, "prior\_cases\_checked": 7, "truncated": false }`

- Prior analysis `08324647-35af-4af2-8d82-4387eec03918` shares 38 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 31 observations. This does not establish a common campaign.
- Prior analysis `7a2cfe72-f48d-4894-8a2d-8889cb3b11b2` shares 47 observations. This does not establish a common campaign.
- Prior analysis `81373b30-6a59-49d1-89b0-bad73ed19eaa` shares 26 observations. This does not establish a common campaign.
- Prior analysis `38851ad7-b3a0-423d-ae89-3b7be4e4b908` shares 26 observations. This does not establish a common campaign.
- Prior analysis `bfccc426-aa9b-4007-8558-a66d37ecb90c` shares 56 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": 6, "exported_objects": 54, "hashed_bytes": 215, "hashed_objects": 54, "omitted_unique_hashes": 0, "returned_unique_hashes": 6, "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": 6 }`. 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 4/4, observables 147/147, artifacts 6/6. Full returned inventory is in the JSON result.