

AdversaryGraph

Threat Intelligence Analysis Report

Analysis Metadata

Provider:	deterministic
Model:	tshark-evidence-v3
Domain:	enterprise-attack
Session ID:	91100160-1a16-4165-bf1d-6b5876fb4e11
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 5880 packets across 27 IP endpoints and 157 transport flows. Observed 88 DNS events, 24 HTTP requests, 24 TLS ClientHello events, and 14 exported HTTP object(s). Deterministic rules produced 8 finding(s): 0 high, 2 medium, and 6 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: 21317 / 21317 characters
Promotion ready: No

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

Promotion blockers

- gate_pending:source_provenance
- gate_pending:publication_date
- gate_pending:procedure_relevance
- gate_pending:procedure_level_claim
- gate_pending:actor_identification
- claims_unresolved:86
- 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: 2022-01-07-traffic-analysis-exercise.pcap

Capture SHA-256: `a86b11ee443ee59d95e4590bdf761235c5d240128d6d195233d065ab57777e8b`

Semantic result SHA-256: `d99f9f0718d2f13b17822949ddc765679358c5ce545ed0bc49ba70534ed25482`

Analyzer manifest SHA-256: `ee952aeb7cdc6958f4ae5178c54c274a1e4f0aec4d42f3bdb95baaff063b3dde`

Executive summary

Decoded 5880 packets across 27 IP endpoints and 157 transport flows. Observed 88 DNS events, 24 HTTP requests, 24 TLS ClientHello events, and 14 exported HTTP object(s). Deterministic rules produced 8 finding(s): 0 high, 2 medium, and 6 low. Findings are evidence-bound candidates and require analyst review; encrypted payload contents remain unavailable.

Capture facts

- Packets: 5880
- Duration: 1172563861.65932 seconds
- Captured bytes: 4628888
- Endpoints: 27
- Flows: 157

Deterministic findings

MEDIUM \u2014 Script, archive, or executable transfer candidate

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

Rule: `script-or-executable-transfer@pcap-rules-v3`; confidence: 0.86; evidence: frame 5309 / TCP stream 76, frame 5315 / TCP stream 76, frame 5317 / TCP stream 76, frame 5636 / TCP stream 76.

Metrics: `{ "content_type": "application/octet-stream", "declared_body_bytes": 307634, "destination": "192.168.1.216", "response_count": 2, "source": "23.38.189.225", "uri": "/c/msdownload/update/software/defu/2022/01/am_delta_patch_1.355.1569.0_f5fe52e10a18f6ce4bc39541e4aae4a97c270c81.exe" }

MEDIUM \u2014 Script, archive, or executable transfer candidate

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

Rule: `script-or-executable-transfer@pcap-rules-v3`; confidence: 0.86; evidence: frame 5313 / TCP stream 77, frame 5316 / TCP stream 77.

Metrics: `{ "content_type": "application/octet-stream", "declared_body_bytes": 2, "destination": "192.168.1.216", "response_count": 1, "source": "23.38.189.201", "uri": "/c/msdownload/update/software/defu/2022/01/am_delta_patch_1.355.1569.0_f5fe52e10a18f6ce4bc39541e4aae4a97c270c81.exe" }

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 246 / TCP stream 6, frame 253 / TCP stream 6, frame 254 / TCP stream 10, frame 257 / TCP stream 6, frame 262 / TCP stream 6.

Metrics: `{ "destination": "192.168.1.216", "event_count": 30, "operation_numbers": ["0", "1", "12", "13", "30"], "protocol": "drsuapi", "source": "192.168.1.2" }

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 191 / TCP stream 15, frame 213 / TCP stream 15, frame 219 / TCP stream 15, frame 221 / TCP stream 15.

Metrics: `{"destination":"192.168.1.216","event\_count":47,"operation\_numbers":["","1","4,19,19,19,5","4,5","5"],"protocol":"ldap","source":"192.168.1.2"}`

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 931 / TCP stream 43, frame 933 / TCP stream 43, frame 935 / TCP stream 43, frame 937 / TCP stream 43, frame 939 / TCP stream 43.

Metrics: `{"destination":"192.168.1.216","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"192.168.1.2"}`

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 241 / TCP stream 6, frame 251 / TCP stream 6, frame 252 / TCP stream 10, frame 255 / TCP stream 6, frame 256 / TCP stream 10.

Metrics: `{"destination":"192.168.1.2","event\_count":30,"operation\_numbers":["0","1","12","13","30"],"protocol":"druapi","source":"192.168.1.216"}`

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 189 / TCP stream 15, frame 210 / TCP stream 15, frame 218 / TCP stream 15, frame 220 / TCP stream 15.

Metrics: `{"destination":"192.168.1.2","event\_count":58,"operation\_numbers":["","0","2","3"],"protocol":"ldap","source":"192.168.1.216"}`

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 930 / TCP stream 43, frame 932 / TCP stream 43, frame 934 / TCP stream 43, frame 936 / TCP stream 43, frame 938 / TCP stream 43.

Metrics: `{"destination":"192.168.1.2","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"192.168.1.216"}`

ATT&CK candidates

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

Identities

- account: `desktop-gxmyno2\$`; client IPs: 192.168.1.216; frames: 75, 108, 126, 127, 129
- account: `steve.smith`; client IPs: 192.168.1.216; frames: 829, 837, 839, 851, 891
- domain: `SPOONWATCH`; client IPs: 192.168.1.216; frames: 914
- full-name: `Steve Smith`; client IPs: 192.168.1.216; frames: 945
- hostname: `DESKTOP-GXMYNO2`; client IPs: 192.168.1.216; frames: 1, 694, 756, 757, 914
- hostname: `DESKTOP-GXNYNO2`; client IPs: 192.168.1.216; frames: 35, 51, 367, 395, 595
- netbios-group: `SPOONWATCH`; client IPs: unbound subject; frames: 34, 366, 581, 596, 598

IOC and artifact candidates

- domain: `api.msn.com`; roles: dns-query, tls-sni
- domain: `au.download.windowsupdate.com`; roles: dns-query, http-host
- domain: `client.wns.windows.com`; roles: dns-query, tls-sni
- domain: `cp801.prod.do.dsp.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `ctldl.windowsupdate.com`; roles: dns-query, http-host
- domain: `dns.msftncsi.com`; roles: dns-query
- domain: `download.windowsupdate.com`; roles: dns-query, http-host
- domain: `fe2cr.update.microsoft.com`; roles: dns-query, tls-sni
- domain: `fe3cr.delivery.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `geo.prod.do.dsp.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `kv801.prod.do.dsp.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `pti.store.microsoft.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: `spoonwatch-dc.spoonwatch.net`; roles: dns-query
- domain: `spoonwatch.net`; roles: dns-query
- domain: `v10.events.data.microsoft.com`; roles: dns-query, tls-sni
- domain: `v20.events.data.microsoft.com`; roles: dns-query, tls-sni
- domain: `wns.notify.trafficmanager.net`; roles: dns-cname
- domain: `wpad.localdomain`; roles: dns-query
- domain: `wpad.spoonwatch.net`; roles: dns-query
- domain: `www.bing.com`; roles: dns-query, tls-sni
- ipv4: `0.0.0.0`; roles: network-endpoint
- ipv4: `104.212.67.47`; roles: dns-answer, network-endpoint
- ipv4: `13.107.21.200`; roles: dns-answer
- ipv4: `131.107.255.255`; roles: dns-answer
- ipv4: `184.50.62.43`; roles: dns-answer, network-endpoint
- ipv4: `192.168.1.1`; roles: network-endpoint
- ipv4: `192.168.1.2`; roles: dns-answer, network-endpoint
- ipv4: `192.168.1.216`; roles: network-endpoint
- ipv4: `192.168.1.255`; roles: network-endpoint
- ipv4: `2.56.57.108`; roles: http-host, network-endpoint
- ipv4: `20.189.173.1`; roles: dns-answer, network-endpoint
- ipv4: `20.50.80.210`; roles: dns-answer, network-endpoint
- ipv4: `20.54.89.15`; roles: dns-answer, network-endpoint
- ipv4: `204.79.197.200`; roles: dns-answer, network-endpoint
- ipv4: `204.79.197.203`; roles: dns-answer, network-endpoint
- ipv4: `224.0.0.22`; roles: network-endpoint
- ipv4: `224.0.0.251`; roles: network-endpoint
- ipv4: `224.0.0.252`; roles: network-endpoint
- ipv4: `23.38.189.201`; roles: dns-answer, network-endpoint
- ipv4: `23.38.189.225`; roles: dns-answer, network-endpoint
- ipv4: `239.255.255.250`; roles: http-host, network-endpoint
- ipv4: `255.255.255.255`; roles: network-endpoint
- ipv4: `40.83.240.146`; roles: dns-answer, network-endpoint
- ipv4: `52.168.112.67`; roles: dns-answer, network-endpoint
- ipv4: `52.178.17.2`; roles: dns-answer, network-endpoint
- ipv4: `52.179.216.235`; roles: dns-answer, network-endpoint
- ipv4: `52.183.220.149`; roles: dns-answer, network-endpoint
- ipv4: `52.238.248.1`; roles: dns-answer
- ipv4: `52.249.36.204`; roles: dns-answer, network-endpoint
- ipv4: `67.27.123.126`; roles: dns-answer
- ipv4: `8.240.136.254`; roles: dns-answer
- ipv4: `8.249.3.254`; roles: dns-answer
- ipv4: `8.249.7.254`; roles: dns-answer
- ipv4: `8.253.189.126`; roles: dns-answer, network-endpoint
- ja3: `28a2c9bd18a11de089ef85a160da29e4`; roles: tls-client-fingerprint
- ja3: `37f463bf4616ecd445d4a1937da06e19`; roles: tls-client-fingerprint
- ja3: `3b5074b1b5d032e5620f69f9f700ff0e`; roles: tls-client-fingerprint
- ja3: `6271f898ce5be7dd52b0fc260d0662b3`; roles: tls-client-fingerprint
- ja3: `a0e9f5d64349fb13191bc781f81f42e1`; roles: tls-client-fingerprint

- sha256: `0cb0222fbde977f15ebc3a7d555ed658763d9a3f507b3f7869416e1b2885adf2`; roles: exported-object

- sha256: `16574f51785b0e2fc29c2c61477eb47bb39f714829999511dc8952b43ab17660`; roles: exported-object

- sha256: `18180895844cba1cd9d310f04e0cfa26cff43b84eebacdc74809edf0e165d082`; roles: exported-object

- sha256: `1ecee6ff37e03c1160b8bf66d5ca8dc784e0b35fb9fd105f0964b314d310c07f`; roles: exported-object

- sha256: `334e69ac9367f708ce601a6f490ff227d6c20636da5222f148b25831d22e13d4`; roles: exported-object

- sha256: `3fe6b1c54b8cf28f571e0c5d6636b4069a8ab00b4f11dd842cfec00691d0c9cd`; roles: exported-object

- sha256: `43536adef2ddcc811c28d35fa6ce3031029a2424ad393989db36169ff2995083`; roles: exported-object

- sha256: `6482cf553a8dd0d2b4812ed1e4916423e9b233e77b3f73e8dcf1e1afdef0d1e9`; roles: exported-object

- sha256: `7b8ab07521c24e8ec610611e7e15d2fd39336166db6509885b8500d2a2bbfb14`; roles: exported-object

- sha256: `835eb064fabd072bd2aa6079f0b0949fbaf6fb677369c1a0cadcec666dbfffc7`; roles: exported-object

- sha256: `9b8db510ef42b8ed54a3712636fda55a4f8cfcd5493e20b74ab00cd4f3979fd`; roles: exported-object

- sha256: `a770ecba3b08bbabd0a567fc978e50615f8b346709f8eb3cfac3faab24090ba`; roles: exported-object

- sha256: `c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d`; roles: exported-object

- sha256: `e2935b5b28550d47dc971f456d6961f20d1633b4892998750140e0eaa9ae9d78`; roles: exported-object

- url: `http://2.56.57.108/osk/`; roles: http-request

- url: `http://2.56.57.108/osk/1.jpg`; roles: http-request

- url: `http://2.56.57.108/osk/2.jpg`; roles: http-request

- url: `http://2.56.57.108/osk/3.jpg`; roles: http-request

- url: `http://2.56.57.108/osk/4.jpg`; roles: http-request

- url: `http://2.56.57.108/osk/5.jpg`; roles: http-request

- url: `http://2.56.57.108/osk/6.jpg`; roles: http-request

- url: `http://2.56.57.108/osk/7.jpg`; roles: http-request

- url: `http://2.56.57.108/osk/main.php`; roles: http-request

- url: `http://239.255.255.250:1900\*`; roles: http-request

- url: `http://au.download.windowsupdate.com/c/msdownload/update/software/defu/2022/01/am\_delta\_patch\_1.355.1569.0\_f5fe52e10a18f6ce4bc39541e4aae4a97c270c81.exe`; roles: http-request

- url: `http://ctdl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?f622d06ddf57408d`; roles: http-request

- url: `http://download.windowsupdate.com/c/msdownload/update/others/2022/01/35969515\_2975e5b79f9857b7a2d7aa07e0d43359735c8e80.cab`; roles: http-request

- url: `http://download.windowsupdate.com/c/msdownload/update/others/2022/01/35969516\_5bcaf676a3e98426394e538836033ea5ce2bb8c3.cab`; roles: http-request

- url: `http://download.windowsupdate.com/c/msdownload/update/others/2022/01/35969632\_c422aaaf8becdd90e50fb6936708c77c7f97631f.cab`; roles: http-request

- user_agent: `Microsoft-CryptoAPI/10.0`; roles: http-client

- user_agent: `Microsoft-Delivery-Optimization/10.0`; roles: http-client

- user_agent: `Windows-Update-Agent/10.0.10011.16384 Client-Protocol/2.32`; roles: http-client

- exported object `5(1).jpg`; SHA-256 `e2935b5b28550d47dc971f456d6961f20d1633b4892998750140e0eaa9ae9d78`; size 1246160 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 `1(1).jpg`; SHA-256 `16574f51785b0e2fc29c2c61477eb47bb39f714829999511dc8952b43ab17660`; size 645592 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 `4(1).jpg`; SHA-256 `334e69ac9367f708ce601a6f490ff227d6c20636da5222f148b25831d22e13d4`; size 440120 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 `2(1).jpg`; SHA-256 `a770ecba3b08bbabd0a567fc978e50615f8b346709f8eb3cfac3faab24090ba`; size 334288 bytes
Static content: `{"content\_kind":"pe","features":[],"inspected\_bytes":262144,"inspection\_truncated":true,"interpretation":"Static content only; not proof of execution, intent, or malware family"}`. Not execution proof.

- exported object `am\_delta\_patch\_1.355.1569.0\_f5fe52e10a18f6ce4bc39541e4aae4a97c270c81(2).exe`; SHA-256 `6482cf553a8dd0d2b4812ed1e4916423e9b233e77b3f73e8dcf1e1afdef0d1e9`; size 307632 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 `6(1).jpg`; SHA-256 `43536adef2ddcc811c28d35fa6ce3031029a2424ad393989db36169ff2995083`; size 144848 bytes
Static content: `{"content\_kind":"pe","features":[{"excerpt":"IEX","feature":"dynamic-evaluation","offset":135147}],inspected\_bytes":144848,"inspection\_truncated":false,"interpretation":"Static content only; not proof of execution, intent, or malware family"}`. Not execution proof.

- exported object `3(1).jpg`; SHA-256 `3fe6b1c54b8cf28f571e0c5d6636b4069a8ab00b4f11dd842cfec00691d0c9cd`; size 137168 bytes
Static content: `{"content\_kind":"pe","features":[{"excerpt":"IEX","feature":"dynamic-evaluation","offset":126724}],inspected\_bytes":137168,"inspection\_truncated":false,"interpretation":"Static content only; not proof of execution, intent, or malware family"}`. Not execution proof.

- exported object `7(1).jpg`; SHA-256 `c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d`; size 83784 bytes
Static content: `{"content\_kind":"pe","features":[],"inspected\_bytes":83784,"inspection\_truncated":false,"interpretation":"Static content only; not proof of execution, intent, or malware family"}`. Not execution proof.

- exported object `osk`; SHA-256 `1ecee6ff37e03c1160b8bf66d5ca8dc784e0b35fb9fd105f0964b314d310c07f`; size 379629 bytes

- exported object `35969632\_c422aaaf8becdd90e50fb6936708c77c7f97631f.cab`; SHA-256 `18180895844cba1cd9d310f04e0cfa26cff43b84eebacdc74809edf0e165d082`; size 10885 bytes

- exported object `35969516\_5bcaf676a3e98426394e538836033ea5ce2bb8c3.cab`; SHA-256 `0cb0222fbde977f15ebc3a7d555ed658763d9a3f

507b3f7869416e1b2885adf2`; size 7317 bytes

- exported object `35969515\_2975e5b79f9857b7a2d7aa07e0d43359735c8e80.cab`; SHA-256 `835eb064fabd072bd2aa6079f0b0949fbaf6fb677369c1a0cadcec666dbfffc7`; size 7313 bytes
- exported object `1.jpg`; SHA-256 `7b8ab07521c24e8ec610611e7e15d2fd39336166db6509885b8500d2a2bbfb14`; size 25 bytes
- exported object `am\_delta\_patch\_1.355.1569.0\_f5fe52e10a18f6ce4bc39541e4aae4a97c270c81(1).exe`; SHA-256 `9b8db510ef42b8ed54a3712636fda55a4f8cfd5493e20b74ab00cd4f3979f2d`; size 2 bytes

Actor similarity leads

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

Local enrichment and correlations

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

Snapshot: `4775c16cd4ef1258e6af0730109f96f3ed0ac43a533ee465dd460c85c852613e`; recorded 2026-09-19T12:09:31.260950+00:00; mode: local-only.

Coverage: `{ "matched\_observables":0, "no\_exact\_match":94, "observable\_limit":5000, "observables\_checked":94, "observables\_total":94, "prior\_case\_limit\_reached":false, "prior\_cases\_checked":12, "truncated":false }`

- Catalog T1105: <https://attack.mitre.org/techniques/T1105>; detection strategies: [{"attack_id":"DET0060","name":"Detect Ingress Tool Transfers via Behavioral Chain","stix_id":"x-mitre-detection-strategy--67677c4c-5778-49eb-ae74-1920645b8554"}]
- Prior analysis `43bc93eb-d6db-4400-b983-b0dd404c8ca4` shares 27 observations. This does not establish a common campaign.
- Prior analysis `6df36b51-4b44-4660-b534-2fa89705e807` shares 18 observations. This does not establish a common campaign.
- Prior analysis `29aa3ef8-47c9-4c47-b4cc-1ff3e0708142` shares 13 observations. This does not establish a common campaign.
- Prior analysis `b79032a8-d69e-4ac1-bdd4-542473fa8e3b` shares 15 observations. This does not establish a common campaign.
- Prior analysis `faf041c3-70e0-4a01-8780-10917e5e187c` shares 14 observations. This does not establish a common campaign.
- Prior analysis `08324647-35af-4af2-8d82-4387eec03918` shares 14 observations. This does not establish a common campaign.
- Prior analysis `616a90fa-f15e-4fcb-8d56-7b8e0eff5785` shares 5 observations. This does not establish a common campaign.
- Prior analysis `459e119d-191f-49e8-85ea-c78f9de41826` shares 18 observations. This does not establish a common campaign.
- Prior analysis `7a2cfe72-f48d-4894-8a2d-8889cb3b11b2` shares 15 observations. This does not establish a common campaign.
- Prior analysis `81373b30-6a59-49d1-89b0-bad73ed19eaa` shares 12 observations. This does not establish a common campaign.
- Prior analysis `38851ad7-b3a0-423d-ae89-3b7be4e4b908` shares 14 observations. This does not establish a common campaign.
- Prior analysis `bfccc426-aa9b-4007-8558-a66d37ecb90c` shares 21 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":14, "exported_objects":22, "hashed_bytes":3744940, "hashed_objects":22, "omitted_unique_hashes":0, "returned_unique_hashes":14, "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":14 }`. 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 7/7, observables 94/94, artifacts 14/14. Full returned inventory is in the JSON result.