

AdversaryGraph

Threat Intelligence Analysis Report

Analysis Metadata

Provider:	deterministic
Model:	tshark-evidence-v3
Domain:	enterprise-attack
Session ID:	ce8cf5b8-2927-4b30-804c-2fedaec840f1
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 11562 packets across 45 IP endpoints and 199 transport flows. Observed 174 DNS events, 10 HTTP requests, 77 TLS ClientHello events, and 2 exported HTTP object(s). Deterministic rules produced 8 finding(s): 1 high, 1 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: 18305 / 18305 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:152
- 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: 2024-07-30-traffic-analysis-exercise.pcap

Capture SHA-256: `c48854c24223cf7b4e9880ea72a21a877e4138e4ce36df7b7656e5c6c4043f68`

Semantic result SHA-256: `58e5064c997e69544c60ecc184cfd57339f05da2cfc2b75e8bf8ed7582621e64`

Analyzer manifest SHA-256: `ee952aeb7cdc6958f4ae5178c54c274a1e4f0aec4d42f3bdb95baaff063b3dde`

Executive summary

Decoded 11562 packets across 45 IP endpoints and 199 transport flows. Observed 174 DNS events, 10 HTTP requests, 77 TLS ClientHello events, and 2 exported HTTP object(s). Deterministic rules produced 8 finding(s): 1 high, 1 medium, and 6 low. Findings are evidence-bound candidates and require analyst review; encrypted payload contents remain unavailable.

Capture facts

- Packets: 11562
- Duration: 585.662377 seconds
- Captured bytes: 11341372
- Endpoints: 45
- Flows: 199

Deterministic findings

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 194 / TCP stream 11, frame 196 / TCP stream 11, frame 198 / TCP stream 11, frame 200 / TCP stream 11, frame 663 / TCP stream 34.

Metrics: `{ "destination": "172.16.1.66", "event\_count": 33, "operation\_numbers": [ "0", "1", "12", "13" ], "protocol": "drsuapi", "source": "172.16.1.4" }`

LOW \u2014 Directory-service protocol activity

Directory protocol operations were decoded. Normal Windows logon uses these protocols; activity alone does not establish discovery, credential theft, or DCSync.

Rule: `directory-service-activity@pcap-rules-v3`; confidence: 0.95; evidence: frame 44 / TCP stream 0, frame 45 / TCP stream 0, frame 49 / TCP stream 1, frame 50 / TCP stream 1, frame 136 / TCP stream 1.

Metrics: `{ "destination": "172.16.1.66", "event\_count": 87, "operation\_numbers": [ "", "1", "4", "4,19,19,19,5", "4,5", "5" ], "protocol": "ldap", "source": "172.16.1.4" }`

LOW \u2014 Directory-service protocol activity

Directory protocol operations were decoded. Normal Windows logon uses these protocols; activity alone does not establish discovery, credential theft, or DCSync.

Rule: `directory-service-activity@pcap-rules-v3`; confidence: 0.95; evidence: frame 1056 / TCP stream 21, frame 1058 / TCP stream 21, frame 1060 / TCP stream 21, frame 1062 / TCP stream 21, frame 1064 / TCP stream 21.

Metrics: `{ "destination": "172.16.1.66", "event\_count": 15, "operation\_numbers": [ "1", "16", "17", "3", "34", "36", "39", "5", "6", "64", "7" ], "protocol": "samr", "source": "172.16.1.4" }`

LOW \u2014 Directory-service protocol activity

Directory protocol operations were decoded. Normal Windows logon uses these protocols; activity alone does not establish discovery, credential theft, or DCSync.

Rule: `directory-service-activity@pcap-rules-v3`; confidence: 0.95; evidence: frame 193 / TCP stream 11, frame 195 / TCP stream 11, frame 197 / TCP stream 11, frame 199 / TCP stream 11, frame 662 / TCP stream 34.

Metrics: `{ "destination": "172.16.1.4", "event\_count": 33, "operation\_numbers": [ "0", "1", "12", "13" ], "protocol": "drsuapi", "source": "172.16.1.66" }`

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 42 / TCP stream 0, frame 46 / TCP stream 1, frame 128 / TCP stream 5, frame 130 / TCP stream 1, frame 133 / TCP stream 0.

Metrics: `{ "destination": "172.16.1.4", "event\_count": 99, "operation\_numbers": [ "0", "2", "3" ], "protocol": "ldap", "source": "172.16.1.66" }`

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 1055 / TCP stream 21, frame 1057 / TCP stream 21, frame 1059 / TCP stream 21, frame 1061 / TCP stream 21, frame 1063 / TCP stream 21.

Metrics: `{ "destination": "172.16.1.4", "event\_count": 15, "operation\_numbers": [ "1", "16", "17", "3", "34", "36", "39", "5", "6", "64", "7" ], "protocol": "samr", "source": "172.16.1.66" }`

HIGH \u2014 Client announces a software label and host identity

An otherwise unclassified TCP payload contains a structured ping, software label, client identifier, hostname and account. These are literal self-reported values, not authenticated identity or independent malware-family attribution.

Rule: `cleartext-tool-self-identification@pcap-rules-v3`; confidence: 0.98; evidence: frame 9119 / TCP stream 83, frame 9352 / TCP stream 83, frame 9530 / TCP stream 83, frame 9537 / TCP stream 83, frame 9563 / TCP stream 83.

Metrics: `{ "claimed\_account": "ccollier", "claimed\_hostname": "DESKTOP-SKBR25F", "client\_id": "1BE8292C", "destination": "141.98.10.79", "destination\_port": 12132, "message\_count": 102, "software\_label": "STRRAT", "source": "172.16.1.66" }`

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 9066 / TCP stream 83.

Metrics: `{ "destination": "141.98.10.79", "destination\_port": 12132, "duration\_seconds": 508.67, "packets": 411, "source": "172.16.1.66", "wire\_bytes": 39064 }`

ATT&CK candidates

- No deterministic ATT&CK candidates.

Identities

- account: `ccollier`; client IPs: 172.16.1.66; frames: 913, 921, 923, 935, 956
- account: `desktop-skbr25f\$`; client IPs: 172.16.1.66; frames: 58, 59, 71, 73, 84
- domain: `WIRESHARKWORKSH`; client IPs: 172.16.1.66; frames: 275
- full-name: `Clark Collier`; client IPs: 172.16.1.66; frames: 1070
- hostname: `DESKTOP-SKBR25F`; client IPs: 172.16.1.66; frames: 29, 30, 275, 499, 500
- netbios-group: `WIRESHARKWORKSH`; client IPs: unbound subject; frames: 31, 501, 615, 616, 624

IOC and artifact candidates

- domain: `a1834.dscg2.akamai.net`; roles: dns-cname
- domain: `api-msn-com.a-0003.a-msedge.net`; roles: dns-cname

- 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: `autodiscover-s.outlook.com`; roles: dns-query, tls-sni
- domain: `autodiscover.wiresharkworkshop.online`; roles: dns-query
- domain: `client.wns.windows.com`; roles: dns-query, tls-sni
- domain: `config.edge.skype.com`; roles: dns-query, tls-sni
- domain: `default.exp-tas.com`; roles: dns-query, tls-sni
- domain: `desktop-skbr25f.wiresharkworkshop.online`; roles: dns-query
- domain: `dualstack.sonatype.map.fastly.net`; roles: dns-cname
- domain: `ecn.dev.virtualearth.net`; roles: dns-query, tls-sni
- domain: `ecs.office.com`; roles: dns-query, tls-sni
- domain: `fd.api.iris.microsoft.com`; roles: dns-query
- domain: `g.live.com`; roles: dns-query, tls-sni
- domain: `github.com`; roles: dns-query, tls-sni
- domain: `go.microsoft.com`; roles: dns-query, tls-sni
- domain: `img-s-msn-com.akamaized.net`; roles: dns-query, tls-sni
- domain: `ip-api.com`; roles: dns-query, http-host
- domain: `javadl-esd-secure.oracle.com`; roles: dns-query, tls-sni
- domain: `login.microsoftonline.com`; roles: dns-query, tls-sni
- domain: `metadata.templates.cdn.office.net`; roles: dns-query, tls-sni
- domain: `mobile.events.data.microsoft.com`; roles: dns-query, tls-sni
- domain: `msedge.api.cdp.microsoft.com`; roles: dns-query, tls-sni
- domain: `objects.githubusercontent.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: `repo1.maven.org`; roles: dns-query, tls-sni
- domain: `settings-win.data.microsoft.com`; roles: dns-query, tls-sni
- domain: `srtb.msn.com`; roles: dns-query, tls-sni
- domain: `th.bing.com`; roles: dns-query, tls-sni
- domain: `v10.events.data.microsoft.com`; roles: dns-query, tls-sni
- domain: `v20.events.data.microsoft.com`; roles: dns-query, tls-sni
- domain: `windows.msn.com`; roles: dns-query, tls-sni
- domain: `wireshark-ws-dc.wiresharkworkshop.online`; roles: dns-query
- domain: `wiresharkworkshop.online`; roles: dns-query
- domain: `wns.notify.trafficmanager.net`; roles: dns-cname
- domain: `wpad.wiresharkworkshop.online`; roles: dns-query
- domain: `www.bing.com`; roles: dns-query, tls-sni
- domain: `www.msftconnecttest.com`; roles: dns-query, http-host
- domain: `www.msn.com`; roles: dns-query, tls-sni
- ipv4: `13.107.42.16`; roles: dns-answer, network-endpoint
- ipv4: `13.107.5.93`; roles: dns-answer, network-endpoint
- ipv4: `13.69.239.79`; roles: dns-answer, network-endpoint
- ipv4: `140.82.113.3`; roles: dns-answer, network-endpoint
- ipv4: `141.98.10.79`; roles: network-endpoint
- ipv4: `172.16.1.255`; roles: network-endpoint
- ipv4: `172.16.1.4`; roles: dns-answer, network-endpoint
- ipv4: `172.16.1.66`; roles: dns-answer, network-endpoint
- ipv4: `185.199.108.133`; roles: dns-answer
- ipv4: `185.199.109.133`; roles: dns-answer
- ipv4: `185.199.110.133`; roles: dns-answer, network-endpoint
- ipv4: `185.199.111.133`; roles: dns-answer
- ipv4: `199.232.192.209`; roles: dns-answer
- ipv4: `199.232.196.209`; roles: dns-answer, network-endpoint
- ipv4: `20.166.2.191`; roles: dns-answer, network-endpoint
- ipv4: `20.189.173.10`; roles: dns-answer, network-endpoint
- ipv4: `20.189.173.16`; roles: dns-answer, network-endpoint
- ipv4: `20.189.173.26`; roles: dns-answer, network-endpoint
- ipv4: `20.190.157.11`; roles: dns-answer
- ipv4: `20.190.157.9`; roles: dns-answer
- ipv4: `20.241.44.114`; roles: dns-answer, network-endpoint
- ipv4: `20.7.1.246`; roles: network-endpoint
- ipv4: `20.7.2.167`; 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: `208.95.112.1`; roles: dns-answer, network-endpoint
- ipv4: `224.0.0.22`; roles: network-endpoint
- ipv4: `224.0.0.251`; roles: network-endpoint
- ipv4: `224.0.0.252`; roles: network-endpoint
- ipv4: `23.194.164.136`; roles: dns-answer, network-endpoint
- ipv4: `23.198.7.167`; roles: dns-answer
- ipv4: `23.198.7.168`; roles: dns-answer, network-endpoint
- ipv4: `23.198.7.169`; roles: dns-answer
- ipv4: `23.198.7.170`; roles: dns-answer
- ipv4: `23.198.7.172`; roles: dns-answer
- ipv4: `23.198.7.173`; roles: dns-answer
- ipv4: `23.198.7.174`; roles: dns-answer
- ipv4: `23.198.7.175`; roles: dns-answer, network-endpoint
- ipv4: `23.198.7.176`; roles: dns-answer
- ipv4: `23.198.7.177`; roles: dns-answer, network-endpoint
- ipv4: `23.198.7.182`; roles: dns-answer
- ipv4: `23.198.7.183`; roles: dns-answer
- ipv4: `23.198.7.186`; roles: dns-answer
- ipv4: `23.215.55.133`; roles: dns-answer, network-endpoint
- ipv4: `23.215.55.137`; roles: dns-answer
- ipv4: `23.215.55.140`; roles: dns-answer, network-endpoint
- ipv4: `23.215.55.144`; roles: dns-answer
- ipv4: `23.221.22.68`; roles: dns-answer, network-endpoint
- ipv4: `23.221.22.87`; roles: dns-answer
- ipv4: `23.46.192.165`; roles: dns-answer, network-endpoint
- ipv4: `23.48.203.199`; roles: dns-answer
- ipv4: `23.48.203.200`; roles: dns-answer
- ipv4: `23.48.203.201`; roles: dns-answer
- ipv4: `23.48.203.203`; roles: dns-answer, network-endpoint
- ipv4: `23.48.203.204`; roles: dns-answer
- ipv4: `23.48.203.205`; roles: dns-answer
- ipv4: `23.48.203.206`; roles: dns-answer
- ipv4: `23.48.203.207`; roles: dns-answer
- ipv4: `23.48.203.208`; roles: dns-answer, network-endpoint
- ipv4: `23.48.203.210`; roles: dns-answer
- ipv4: `23.52.9.140`; roles: dns-answer, network-endpoint
- ipv4: `23.52.9.222`; roles: dns-answer, network-endpoint
- ipv4: `23.53.11.164`; roles: dns-answer
- ipv4: `23.53.11.165`; roles: dns-answer
- ipv4: `23.53.11.166`; roles: dns-answer, network-endpoint
- ipv4: `23.53.11.174`; roles: dns-answer
- ipv4: `23.53.11.175`; roles: dns-answer
- ipv4: `23.53.11.176`; roles: dns-answer
- ipv4: `23.53.11.177`; roles: dns-answer
- ipv4: `23.53.11.178`; roles: dns-answer
- ipv4: `23.53.11.179`; roles: dns-answer
- ipv4: `23.96.180.189`; roles: dns-answer
- ipv4: `239.255.255.250`; roles: http-host, network-endpoint
- ipv4: `40.126.29.11`; roles: dns-answer
- ipv4: `40.126.29.13`; roles: dns-answer
- ipv4: `40.126.29.14`; roles: dns-answer, network-endpoint
- ipv4: `40.126.29.5`; roles: dns-answer
- ipv4: `40.126.29.7`; roles: dns-answer
- ipv4: `40.126.29.8`; roles: dns-answer
- ipv4: `40.97.199.114`; roles: dns-answer, network-endpoint
- ipv4: `40.99.169.130`; roles: dns-answer
- ipv4: `52.109.0.142`; roles: dns-answer, network-endpoint
- ipv4: `52.109.0.91`; roles: dns-answer, network-endpoint
- ipv4: `52.109.20.47`; roles: dns-answer, network-endpoint
- ipv4: `52.109.6.53`; roles: dns-answer, network-endpoint
- ipv4: `52.113.194.132`; roles: dns-answer, network-endpoint
- ipv4: `52.191.219.104`; roles: dns-answer, network-endpoint
- ipv4: `52.96.121.130`; roles: dns-answer

- ipv4: `52.96.57.2`; roles: dns-answer
- ja3: `026e5ca865ce1f09da3a81d8a4e3effb`; roles: tls-client-fingerprint
- ja3: `091f51a7a1c3a4504a224cc081ce9cee`; roles: tls-client-fingerprint
- ja3: `1541459f873df5079e5cf7ff2c951ca0`; roles: tls-client-fingerprint
- ja3: `17e7f892bd0cb5409482f240c9ca2934`; roles: tls-client-fingerprint
- ja3: `1968767952a7e119234b43165830caaf`; roles: tls-client-fingerprint
- ja3: `258a5a1e95b8a911872bae9081526644`; roles: tls-client-fingerprint
- ja3: `292a36e182b3281950ca910a639428ec`; roles: tls-client-fingerprint
- ja3: `3c293bdf2a25c07559b560ba86debc77`; roles: tls-client-fingerprint
- ja3: `3c4eb72b882d4d1442c67ce73f1292a9`; roles: tls-client-fingerprint
- ja3: `46f5131e766d248db0248a86c494b71c`; roles: tls-client-fingerprint
- ja3: `54e118fb6c893793f9955efcc86a6132`; roles: tls-client-fingerprint
- ja3: `65005c9d9ae0f0e0beaf22c210571d482`; roles: tls-client-fingerprint
- ja3: `6764675c1ca709250abb58a1ed36b1a9`; roles: tls-client-fingerprint
- ja3: `6a5d235ee78c6aede6a61448b4e9ff1e`; roles: tls-client-fingerprint
- ja3: `6d162fd4fcafeafc279a32732bb583ab`; roles: tls-client-fingerprint
- ja3: `7dcea60ae4f829abcfa00bd64ab6f937`; roles: tls-client-fingerprint
- ja3: `930a922a3aeaa3a5590435675e8a4bb9`; roles: tls-client-fingerprint
- sha256: `47729774d301b648e88dee3b5e215d63adabb069700e1d81671fcbdfb80e4bb`; roles: exported-object
- sha256: `5e9a7996fe94d7be10595d7133748760bf8348198b71b7a50fd8affaa980ac61`; roles: exported-object
- url: `http://239.255.255.250:1900\*`; roles: http-request
- url: `http://ip-api.com/json/`; roles: http-request
- url: `http://www.msftconnecttest.com/connecttest.txt`; roles: http-request
- user_agent: `Microsoft NCSI`; roles: http-client
- user_agent: `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36`; role: http-client
- exported object `json`; SHA-256 `47729774d301b648e88dee3b5e215d63adabb069700e1d81671fcbdfb80e4bb`; size 294 bytes
- exported object `connecttest.txt`; SHA-256 `5e9a7996fe94d7be10595d7133748760bf8348198b71b7a50fd8affaa980ac61`; size 22 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: `32e9d5fcf77c5a465a8b3ffc21d77a172a52a6eb0c40ad986ced99d0994dd0d3`; recorded 2026-09-19T12:09:03.146463+00:00; mode: local-only.

Coverage: `{"matched\_observables":0,"no\_exact\_match":157,"observable\_limit":5000,"observables\_checked":157,"observables\_total":157,"prior\_case\_limit\_reached":false,"prior\_cases\_checked":9,"truncated":false}`

- Prior analysis `b79032a8-d69e-4ac1-bdd4-542473fa8e3b` shares 45 observations. This does not establish a common campaign.
- Prior analysis `faf041c3-70e0-4a01-8780-10917e5e187c` shares 33 observations. This does not establish a common campaign.
- Prior analysis `08324647-35af-4af2-8d82-4387eec03918` shares 33 observations. This does not establish a common campaign.
- Prior analysis `616a90fa-f15e-4fcb-8d56-7b8e0eff5785` shares 11 observations. This does not establish a common campaign.
- Prior analysis `459e119d-191f-49e8-85ea-c78f9de41826` shares 27 observations. This does not establish a common campaign.
- Prior analysis `7a2cfe72-f48d-4894-8a2d-8889cb3b11b2` shares 37 observations. This does not establish a common campaign.
- Prior analysis `81373b30-6a59-49d1-89b0-bad73ed19eaa` shares 31 observations. This does not establish a common campaign.
- Prior analysis `38851ad7-b3a0-423d-ae89-3b7be4e4b908` shares 35 observations. This does not establish a common campaign.
- Prior analysis `bfccc426-aa9b-4007-8558-a66d37ecb90c` shares 48 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":2,"exported_objects":2,"hashed_bytes":316,"hashed_objects":2,"omitted_unique_hashes":0,"returned_unique_hashes":2,"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":2}`. 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 6/6, observables 157/157, artifacts 2/2. Full returned inventory is in the JSON result.