

AdversaryGraph

Threat Intelligence Analysis Report

Analysis Metadata

Provider:	deterministic
Model:	tshark-evidence-v3
Domain:	enterprise-attack
Session ID:	2571013a-e926-41d7-b13c-b180a0720a96
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 16296 packets across 63 IP endpoints and 837 transport flows. Observed 640 DNS events, 38 HTTP requests, 313 TLS ClientHello events, and 2 exported HTTP object(s). Deterministic rules produced 8 finding(s): 0 high, 0 medium, and 8 low. Findings are evidence-bound candidates and require analyst review; encrypted payload contents remain unavailable.

Review Gate Assessment

State: draft
Profile: internal_ir
Revision: 1
Policy: report-review-policy-v1.0
Coverage: 18130 / 18130 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:128
- 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: 2022-03-21-traffic-analysis-exercise.pcap

Capture SHA-256: `d9b67e18bca13cf6135874fd81d167403c7cb6b8a422679948db914e9959b90d`

Semantic result SHA-256: `f38dc6eb2db7e16e10a92b68527beec8e2509ef67cf4ab5380a35fc1909d09af`

Analyzer manifest SHA-256: `ee952aeb7cdc6958f4ae5178c54c274a1e4f0aec4d42f3bdb95baaff063b3dde`

Executive summary

Decoded 16296 packets across 63 IP endpoints and 837 transport flows. Observed 640 DNS events, 38 HTTP requests, 313 TLS ClientHello events, and 2 exported HTTP object(s). Deterministic rules produced 8 finding(s): 0 high, 0 medium, and 8 low. Findings are evidence-bound candidates and require analyst review; encrypted payload contents remain unavailable.

Capture facts

- Packets: 16296
- Duration: 22746.472749 seconds
- Captured bytes: 6591621
- Endpoints: 63
- Flows: 837

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 3298, frame 3584, frame 3845, frame 3916, frame 4014.

Metrics: `{ "domain": "wpad.burnincandle.com", "response\_count": 42, "source": "10.0.19.14" }`

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 3300, frame 3586, frame 3851, frame 3918, frame 4016.

Metrics: `{ "domain": "wpad.mshome.net", "response\_count": 41, "source": "10.0.19.14" }`

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 3450 / TCP stream 23, frame 3452 / TCP stream 23, frame 3454 / TCP stream 23, frame 3458 / TCP stream 23, frame 3460 / TCP stream 23.

Metrics: `{ "destination": "10.0.19.9", "event\_count": 82, "operation\_numbers": [ "0", "1", "12" ], "protocol": "drsuapi", "source": "10.0.19.14" }`

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 3473 / TCP stream 24, frame 3478 / TCP stream 24, frame 3481 / TCP stream 24, frame 3483 / TCP stream 24, frame 3485 / TCP stream 24.

Metrics: `{"destination":"10.0.19.9","event\_count":182,"operation\_numbers":["0","2","3"],"protocol":"ldap","source":"10.0.19.14"}`

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 816 / TCP stream 12, frame 818 / TCP stream 12, frame 820 / TCP stream 12, frame 822 / TCP stream 12, frame 824 / TCP stream 12.

Metrics: `{"destination":"10.0.19.9","event\_count":51,"operation\_numbers":["1","16","17","18","19","20","25","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"10.0.19.14"}`

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 3451 / TCP stream 23, frame 3453 / TCP stream 23, frame 3455 / TCP stream 23, frame 3459 / TCP stream 23, frame 3461 / TCP stream 23.

Metrics: `{"destination":"10.0.19.14","event\_count":82,"operation\_numbers":["0","1","12"],"protocol":"druapi","source":"10.0.19.9"}`

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 3475 / TCP stream 24, frame 3480 / TCP stream 24, frame 3482 / TCP stream 24, frame 3484 / TCP stream 24, frame 3486 / TCP stream 24.

Metrics: `{"destination":"10.0.19.14","event\_count":146,"operation\_numbers":["1","4,19,19,19,5","4,4,4,5","4,5","5"],"protocol":"ldap","source":"10.0.19.9"}`

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 817 / TCP stream 12, frame 819 / TCP stream 12, frame 821 / TCP stream 12, frame 823 / TCP stream 12, frame 825 / TCP stream 12.

Metrics: `{"destination":"10.0.19.14","event\_count":51,"operation\_numbers":["1","16","17","18","19","20","25","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"10.0.19.9"}`

ATT&CK candidates

- No deterministic ATT&CK candidates.

Identities

- account: `DESKTOP-5QS3D5D`; client IPs: 10.0.19.14; frames: 12633, 12641, 12643, 12655, 15402
- account: `patrick.zimmerman`; client IPs: 10.0.19.14; frames: 3696, 4150, 4162, 4171, 4173
- full-name: `Patrick Zimmerman`; client IPs: 10.0.19.14; frames: 3696, 4317
- hostname: `BURNINCANDLE`; client IPs: 10.0.19.14, 169.254.179.89; frames: 3763, 3764, 3765, 3766, 3933
- hostname: `BURNINCANDLE-DC`; client IPs: 10.0.19.9; frames: 3980
- hostname: `DESKTOP-5QS3D5D`; client IPs: 10.0.19.14, 169.254.179.89; frames: 3771, 3773, 744, 3241, 3513
- netbios-group: `BURNINCANDLE`; client IPs: unbound subject; frames: 3724, 3728, 3732, 3735, 3737

IOC and artifact candidates

- domain: `antnosience.com`; roles: dns-query, tls-sni
- domain: `api.msn.com`; roles: dns-query, tls-sni
- domain: `arc.msn.com`; roles: dns-query, tls-sni
- domain: `bupdater.com`; roles: dns-query, tls-sni

- domain: `burnincandle-dc.burnincandle.com`; roles: dns-query
- domain: `checkappexec.microsoft.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: `ctdl.windowsupdate.com`; roles: dns-query, http-host
- domain: `desktop-lr77s6e.burnincandle.com`; roles: dns-query
- domain: `dillmoretast.com`; roles: dns-query, tls-sni
- domain: `dns.msftncsi.com`; roles: dns-query
- domain: `ecs.office.com`; roles: dns-query, tls-sni
- domain: `filebin.net`; roles: dns-query, tls-sni
- domain: `fp-vp-nocache.azureedge.net`; roles: dns-query, tls-sni
- domain: `fp-vp.azureedge.net`; roles: dns-query, tls-sni
- domain: `fp-vs-nocache.azureedge.net`; roles: dns-query, tls-sni
- domain: `licensing.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `login.microsoftonline.com`; roles: dns-query, tls-sni
- domain: `msedge.api.cdp.microsoft.com`; roles: dns-query, tls-sni
- domain: `nexusrules.officeapps.live.com`; roles: dns-query, tls-sni
- domain: `oceriesfornot.top`; roles: http-host
- domain: `otectagain.top`; roles: dns-query, tls-sni
- domain: `prod.nexusrules.live.com.akadns.net`; roles: dns-cname
- domain: `r3.i.lencr.org`; roles: dns-query, http-host
- domain: `seaskysafe.com`; roles: dns-query, tls-sni
- domain: `settings-win.data.microsoft.com`; roles: dns-query, tls-sni
- domain: `situla.bitbit.net`; roles: dns-query, tls-sni
- domain: `spo-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `storecatalogrevocation.storequality.microsoft.com`; roles: dns-query, tls-sni
- domain: `suncoastpinball.com`; roles: dns-query, tls-sni
- domain: `t-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `teams-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `v10.events.data.microsoft.com`; roles: dns-query, tls-sni
- domain: `wns.notify.trafficmanager.net`; roles: dns-cname
- domain: `wpad.burnincandle.com`; roles: dns-query
- domain: `wpad.mshome.net`; roles: dns-query
- domain: `www.bing.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: `10.0.19.1`; roles: network-endpoint
- ipv4: `10.0.19.14`; roles: network-endpoint
- ipv4: `10.0.19.255`; roles: network-endpoint
- ipv4: `10.0.19.9`; roles: dns-answer, network-endpoint
- ipv4: `104.80.96.219`; roles: dns-answer, network-endpoint
- ipv4: `13.107.136.254`; roles: dns-answer, network-endpoint
- ipv4: `13.107.21.200`; roles: dns-answer
- ipv4: `13.107.246.254`; roles: dns-answer, network-endpoint
- ipv4: `13.107.42.16`; roles: dns-answer, network-endpoint
- ipv4: `13.69.116.104`; roles: dns-answer, network-endpoint
- ipv4: `13.69.239.74`; roles: dns-answer, network-endpoint
- ipv4: `13.87.188.105`; 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: `131.107.255.255`; roles: dns-answer
- ipv4: `157.245.142.66`; roles: dns-answer, network-endpoint
- ipv4: `160.153.32.99`; roles: dns-answer, network-endpoint
- ipv4: `169.254.179.89`; roles: network-endpoint
- ipv4: `169.254.255.255`; roles: network-endpoint
- ipv4: `184.85.64.91`; roles: dns-answer, network-endpoint
- ipv4: `185.47.40.36`; roles: dns-answer, network-endpoint
- ipv4: `188.166.154.118`; roles: network-endpoint
- ipv4: `20.189.173.15`; roles: dns-answer, network-endpoint
- ipv4: `20.189.173.2`; roles: dns-answer, network-endpoint
- ipv4: `20.190.154.137`; roles: dns-answer
- ipv4: `20.190.154.139`; roles: dns-answer
- ipv4: `20.190.154.16`; roles: dns-answer
- ipv4: `20.190.154.17`; roles: dns-answer
- ipv4: `20.190.154.18`; roles: dns-answer

- ipv4: `20.190.154.19`; roles: dns-answer
- ipv4: `20.42.65.89`; roles: dns-answer, network-endpoint
- ipv4: `20.44.10.123`; roles: dns-answer, network-endpoint
- ipv4: `20.69.130.185`; roles: dns-answer, network-endpoint
- ipv4: `20.72.205.209`; roles: dns-answer, network-endpoint
- ipv4: `20.81.51.95`; roles: dns-answer, network-endpoint
- ipv4: `20.81.52.156`; 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: `209.197.3.8`; 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: `23.219.38.10`; roles: dns-answer, network-endpoint
- ipv4: `23.219.38.40`; roles: dns-answer
- ipv4: `23.227.198.203`; roles: dns-answer, network-endpoint
- ipv4: `239.255.255.250`; roles: http-host, network-endpoint
- ipv4: `255.255.255.255`; roles: network-endpoint
- ipv4: `40.124.168.44`; roles: dns-answer, network-endpoint
- ipv4: `40.126.26.134`; roles: dns-answer, network-endpoint
- ipv4: `40.126.26.135`; roles: dns-answer
- ipv4: `40.74.98.194`; roles: dns-answer, network-endpoint
- ipv4: `40.83.240.146`; roles: dns-answer, network-endpoint
- ipv4: `51.105.71.137`; roles: dns-answer, network-endpoint
- ipv4: `52.109.8.19`; roles: dns-answer, network-endpoint
- ipv4: `52.109.8.20`; roles: dns-answer, network-endpoint
- ipv4: `52.109.8.21`; roles: dns-answer, network-endpoint
- ipv4: `52.113.194.132`; roles: dns-answer, network-endpoint
- ipv4: `52.113.196.254`; roles: dns-answer, network-endpoint
- ipv4: `52.137.108.250`; roles: dns-answer, network-endpoint
- ipv4: `52.168.117.170`; roles: dns-answer, network-endpoint
- ipv4: `52.182.143.208`; 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: `68.142.107.1`; roles: dns-answer, network-endpoint
- ipv4: `68.142.107.129`; roles: dns-answer, network-endpoint
- ipv4: `69.28.162.0`; roles: dns-answer, network-endpoint
- ipv4: `69.28.162.128`; roles: dns-answer, network-endpoint
- ipv4: `72.21.81.200`; roles: dns-answer, network-endpoint
- ipv4: `72.21.81.240`; roles: dns-answer, network-endpoint
- ipv4: `87.238.33.7`; roles: dns-answer
- ipv4: `87.238.33.8`; roles: dns-answer, network-endpoint
- ipv4: `91.193.16.181`; 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: `67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd`; roles: exported-object
- sha256: `ac64292e91738bf97842e7e5d28373a3a52bdb0aa2bc48a0df512e34d1b41501`; roles: exported-object
- url: `http://239.255.255.250:1900\*`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?161b4282e13b6962`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?48e7354130cbe0e4`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?c66ea67221454a2e`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?c6c9c220471a286c`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?0356947035b28e34`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?1131f2daab4034ba`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8fd0590036de0ddd`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?36a063424dfa7851`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?416ee1a6826abea5`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?9770388e0c613755`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?d1adc478adff0d72`; roles: http-request
- url: `http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?fcfd7669d19bb421`; roles: http-request
- url: `http://oceriesfornot.top/`; roles: http-request

```
- url: `http://r3.i.lencr.org/`; roles: http-request
- url: `http://x1.c.lencr.org/`; roles: http-request
- user_agent: `Microsoft-CryptoAPI/10.0`; roles: http-client
- exported object `%2f`; SHA-256 `ac64292e91738bf97842e7e5d28373a3a52bdb0aa2bc48a0df512e34d1b41501`; size 393277 bytes
- exported object `%2f(1)`; SHA-256 `67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd`; size 1306 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: `6a2316caee77621222da55a0117f143ac0b4ad630ec057912dd940e824fe529d`; recorded 2026-09-19T12:09:11.063080+00:00; mode: local-only.

Coverage: `{ "matched\_observables":0, "no\_exact\_match":137, "observable\_limit":5000, "observables\_checked":137, "observables\_total":137, "prior\_case\_limit\_reached":false, "prior\_cases\_checked":10, "truncated":false }`

- Prior analysis `29aa3ef8-47c9-4c47-b4cc-1ff3e0708142` shares 18 observations. This does not establish a common campaign.
- Prior analysis `b79032a8-d69e-4ac1-bdd4-542473fa8e3b` shares 17 observations. This does not establish a common campaign.
- Prior analysis `faf041c3-70e0-4a01-8780-10917e5e187c` shares 18 observations. This does not establish a common campaign.
- Prior analysis `08324647-35af-4af2-8d82-4387eec03918` shares 19 observations. This does not establish a common campaign.
- Prior analysis `616a90fa-f15e-4fcb-8d56-7b8e0eff5785` shares 4 observations. This does not establish a common campaign.
- Prior analysis `459e119d-191f-49e8-85ea-c78f9de41826` shares 14 observations. This does not establish a common campaign.
- Prior analysis `7a2cfe72-f48d-4894-8a2d-8889cb3b11b2` shares 22 observations. This does not establish a common campaign.
- Prior analysis `81373b30-6a59-49d1-89b0-bad73ed19eaa` shares 16 observations. This does not establish a common campaign.
- Prior analysis `38851ad7-b3a0-423d-ae89-3b7be4e4b908` shares 19 observations. This does not establish a common campaign.
- Prior analysis `bfccc426-aa9b-4007-8558-a66d37ecb90c` shares 19 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":394583, "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 7/7, observables 137/137, artifacts 2/2. Full returned inventory is in the JSON result.