

AdversaryGraph

Threat Intelligence Analysis Report

Analysis Metadata

Provider:	deterministic
Model:	tshark-evidence-v3
Domain:	enterprise-attack
Session ID:	bfa8693a-227f-4f5d-8e70-aff8c425ac42
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 30023 packets across 143 IP endpoints and 809 transport flows. Observed 499 DNS events, 43 HTTP requests, 111 TLS ClientHello events, and 500 exported HTTP object(s). Deterministic rules produced 57 finding(s): 0 high, 39 medium, and 18 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 / 100258 characters
Promotion ready: No

#	Gate	Machine	Analyst	Reason
1	Source provenance	warning	pending	
2	Publication date	fail	pending	
3	Procedure relevance	warning	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:201
- 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: 2022-02-23-traffic-analysis-exercise.pcap

Capture SHA-256: `eefc7e61b50e7846f5a3282d7645539d7b2b4b85aa08a09d0b823896c9449d1f`

Semantic result SHA-256: `8a329890ed01eedca67808c92bdfa492463b036b435540749e5ff2e599d7deee`

Analyzer manifest SHA-256: `ee952aeb7cdc6958f4ae5178c54c274a1e4f0aec4d42f3bdb95baaff063b3dde`

Executive summary

Decoded 30023 packets across 143 IP endpoints and 809 transport flows. Observed 499 DNS events, 43 HTTP requests, 111 TLS ClientHello events, and 500 exported HTTP object(s). Deterministic rules produced 57 finding(s): 0 high, 39 medium, and 18 low. Findings are evidence-based and require analyst review; encrypted payload contents remain unavailable.

Capture facts

- Packets: 30023
- Duration: 2680.736661 seconds
- Captured bytes: 19277433
- Endpoints: 143
- Flows: 809

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 3995 / TCP stream 186, frame 4675 / TCP stream 186.

Metrics: `{ "content\_type": "application/x-msdownload", "declared\_body\_bytes": 593920, "destination": "172.16.0.149", "response\_count": 1, "source": "64.34.171.228", "uri": "/c7g8t/zbBYgukXYxzAF2hZc/" }`

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 178 / TCP stream 8, frame 180 / TCP stream 8, frame 182 / TCP stream 8, frame 184 / TCP stream 8, frame 1710 / TCP stream 8.

Metrics: `{ "destination": "172.16.0.52", "event\_count": 8, "operation\_numbers": [ "0", "1", "12" ], "protocol": "drsuapi", "source": "172.16.0.131" }`

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 100 / TCP stream 5, frame 117 / TCP stream 5, frame 120 / TCP stream 5, frame 212 / TCP stream 13, frame 229 / TCP stream 13.

Metrics: `{ "destination": "172.16.0.52", "event\_count": 41, "operation\_numbers": [ "", "0", "2", "3" ], "protocol": "ldap", "source": "172.16.0.131" }`

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 1785 / TCP stream 87, frame 1787 / TCP stream 87, frame

1790 / TCP stream 87, frame 1793 / TCP stream 87, frame 1795 / TCP stream 87.

Metrics: `{"destination":"172.16.0.52","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"172.16.0.131"}`

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 2143 / TCP stream 101, frame 2159 / TCP stream 101, frame 2162 / TCP stream 101, frame 2168 / TCP stream 101, frame 2214 / TCP stream 111.

Metrics: `{"destination":"172.16.0.52","event\_count":53,"operation\_numbers":["0","1","12","13"],"protocol":"drsuapi","source":"172.16.0.149"}`

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 1944 / TCP stream 94, frame 2015 / TCP stream 94, frame 2018 / TCP stream 94, frame 2055 / TCP stream 102, frame 2091 / TCP stream 102.

Metrics: `{"destination":"172.16.0.52","event\_count":103,"operation\_numbers":["","0","2","3"],"protocol":"ldap","source":"172.16.0.149"}`

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 2867 / TCP stream 95, frame 2869 / TCP stream 95, frame 2871 / TCP stream 95, frame 2873 / TCP stream 95, frame 2875 / TCP stream 95.

Metrics: `{"destination":"172.16.0.52","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"172.16.0.149"}`

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 746 / TCP stream 43, frame 748 / TCP stream 43, frame 750 / TCP stream 43, frame 752 / TCP stream 43, frame 784 / TCP stream 45.

Metrics: `{"destination":"172.16.0.52","event\_count":53,"operation\_numbers":["0","1","12","13"],"protocol":"drsuapi","source":"172.16.0.170"}`

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 577 / TCP stream 32, frame 618 / TCP stream 35, frame 673 / TCP stream 35, frame 682 / TCP stream 35, frame 684 / TCP stream 35.

Metrics: `{"destination":"172.16.0.52","event\_count":98,"operation\_numbers":["","0","2","3"],"protocol":"ldap","source":"172.16.0.170"}`

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 1424 / TCP stream 31, frame 1430 / TCP stream 31, frame 1435 / TCP stream 31, frame 1437 / TCP stream 31, frame 1439 / TCP stream 31.

Metrics: `{"destination":"172.16.0.52","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"172.16.0.131"}`

source":"172.16.0.170"}`

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 179 / TCP stream 8, frame 181 / TCP stream 8, frame 183 / TCP stream 8, frame 185 / TCP stream 8, frame 1711 / TCP stream 8.

Metrics: `{"destination":"172.16.0.131","event\_count":8,"operation\_numbers":["0","1","12"],"protocol":"drsuapi","source":"172.16.0.52"}`

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 102 / TCP stream 5, frame 119 / TCP stream 5, frame 214 / TCP stream 13, frame 231 / TCP stream 13, frame 233 / TCP stream 13.

Metrics: `{"destination":"172.16.0.131","event\_count":33,"operation\_numbers":["","1","4,19,19,19,5","4,5","5"],"protocol":"ldap","source":"172.16.0.52"}`

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 1786 / TCP stream 87, frame 1788 / TCP stream 87, frame 1792 / TCP stream 87, frame 1794 / TCP stream 87, frame 1796 / TCP stream 87.

Metrics: `{"destination":"172.16.0.131","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"172.16.0.52"}`

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 2147 / TCP stream 101, frame 2161 / TCP stream 101, frame 2164 / TCP stream 101, frame 2169 / TCP stream 101, frame 2215 / TCP stream 111.

Metrics: `{"destination":"172.16.0.149","event\_count":53,"operation\_numbers":["0","1","12","13"],"protocol":"drsuapi","source":"172.16.0.52"}`

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 1946 / TCP stream 94, frame 2017 / TCP stream 94, frame 2057 / TCP stream 102, frame 2093 / TCP stream 102, frame 2099 / TCP stream 102.

Metrics: `{"destination":"172.16.0.149","event\_count":83,"operation\_numbers":["","1","4,19,19,19,5","4,5","5"],"protocol":"ldap","source":"172.16.0.52"}`

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 2868 / TCP stream 95, frame 2870 / TCP stream 95, frame 2872 / TCP stream 95, frame 2874 / TCP stream 95, frame 2876 / TCP stream 95.

Metrics: `{"destination":"172.16.0.149","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"172.16.0.52"}`

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 747 / TCP stream 43, frame 749 / TCP stream 43, frame 751 / TCP stream 43, frame 753 / TCP stream 43, frame 785 / TCP stream 45.

Metrics: `{"destination":"172.16.0.170","event\_count":53,"operation\_numbers":["0","1","12","13"],"protocol":"drsuapi","source":"172.16.0.52"}`

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 579 / TCP stream 32, frame 620 / TCP stream 35, frame 681 / TCP stream 35, frame 683 / TCP stream 35, frame 686 / TCP stream 35.

Metrics: `{"destination":"172.16.0.170","event\_count":79,"operation\_numbers":["","1","4,19,19,19,5","4,5","5"],"protocol":"ldap","source":"172.16.0.52"}`

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 1427 / TCP stream 31, frame 1433 / TCP stream 31, frame 1436 / TCP stream 31, frame 1438 / TCP stream 31, frame 1440 / TCP stream 31.

Metrics: `{"destination":"172.16.0.170","event\_count":15,"operation\_numbers":["1","16","17","3","34","36","39","5","6","64","7"],"protocol":"samr","source":"172.16.0.52"}`

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 4679 / TCP stream 187.

Metrics: `{"destination":"135.148.121.246","destination\_port":8080,"duration\_seconds":52.845,"packets":127,"source":"172.16.0.149","wire\_bytes":87055}`

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 4802 / TCP stream 188.

Metrics: `{"destination":"135.148.121.246","destination\_port":8080,"duration\_seconds":96.025,"packets":19,"source":"172.16.0.149","wire\_bytes":2721}`

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 5068 / TCP stream 198.

Metrics: `{"destination":"135.148.121.246","destination\_port":8080,"duration\_seconds":47.78,"packets":19,"source":"172.16.0.149","wire\_bytes":2517}`

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 6688 / TCP stream 203.

Metrics: `{"destination":"27.254.174.84","destination\_port":8080,"duration\_seconds":60.005,"packets":117,"source":"172.16.0.170","wire\_bytes":86156}`

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 6805 / TCP stream 204.

Metrics: `{"destination":"27.254.174.84","destination\_port":8080,"duration\_seconds":104.051,"packets":20,"source":"172.16.0.170","wire\_bytes":3034}`

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 7688 / TCP stream 213.

Metrics: `{"destination":"27.254.174.84","destination\_port":8080,"duration\_seconds":49.984,"packets":18,"source":"172.16.0.170","wire\_bytes":2793}`

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 7719 / TCP stream 214.

Metrics: `{"destination":"135.148.121.246","destination\_port":8080,"duration\_seconds":46.582,"packets":19,"source":"172.16.0.149","wire\_bytes":2755}`

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 7792 / TCP stream 216.

Metrics: `{"destination":"27.254.174.84","destination\_port":8080,"duration\_seconds":41.718,"packets":76,"source":"172.16.0.170","wire\_bytes":54377}`

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 8729 / TCP stream 221.

Metrics: `{"destination":"135.148.121.246","destination\_port":8080,"duration\_seconds":51.375,"packets":412,"source":"172.16.0.149","wire\_bytes":320581}`

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 9146 / TCP stream 222.

Metrics: `{"destination":"135.148.121.246","destination\_port":8080,"duration\_seconds":76.16,"packets":19,"source":"172.16.0.149","wire\_bytes":3342}`

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 9331 / TCP stream 227.

Metrics: `{"destination":"168.197.250.14","destination\_port":80,"duration\_seconds":117.001,"packets":559,"source":"172.16.0.170","wire\_bytes":492888}`

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 10803 / TCP stream 236.

Metrics: `{"destination":"168.197.250.14","destination\_port":80,"duration\_seconds":66.043,"packets":21,"source":"172.16.0.170","wire\_bytes":3237}`

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 10835 / TCP stream 237.

Metrics: `{"destination":"135.148.121.246","destination\_port":8080,"duration\_seconds":61.284,"packets":117,"source":"172.16.0.149","wire\_bytes":89737}`

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 10946 / TCP stream 238.

Metrics: `{"destination":"135.148.121.246","destination\_port":8080,"duration\_seconds":61.474,"packets":21,"source":"172.16.0.149","wire\_bytes":3151}`

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 11650 / TCP stream 247.

Metrics: `{"destination":"135.148.121.246","destination\_port":8080,"duration\_seconds":46.562,"packets":412,"source":"172.16.0.149","wire\_bytes":340415}`

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 11743 / TCP stream 249.

Metrics: `{"destination":"168.197.250.14","destination\_port":80,"duration\_seconds":95.062,"packets":19,"source":"172.16.0.170","wire\_bytes":2986}`

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 12139 / TCP stream 251.

Metrics: `{ "destination": "135.148.121.246", "destination\_port": 8080, "duration\_seconds": 44.834, "packets": 19, "source": "172.16.0.149", "wire\_bytes": 3271 }`

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 13103 / TCP stream 261.

Metrics: `{ "destination": "135.148.121.246", "destination\_port": 8080, "duration\_seconds": 48.149, "packets": 19, "source": "172.16.0.149", "wire\_bytes": 2678 }`

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 13119 / TCP stream 262.

Metrics: `{ "destination": "168.197.250.14", "destination\_port": 80, "duration\_seconds": 79.426, "packets": 19, "source": "172.16.0.170", "wire\_bytes": 3058 }`

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 13219 / TCP stream 268.

Metrics: `{ "destination": "168.197.250.14", "destination\_port": 80, "duration\_seconds": 94.94, "packets": 398, "source": "172.16.0.170", "wire\_bytes": 319970 }`

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 13452 / TCP stream 272.

Metrics: `{ "destination": "135.148.121.246", "destination\_port": 8080, "duration\_seconds": 49.955, "packets": 132, "source": "172.16.0.149", "wire\_bytes": 101806 }`

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 13684 / TCP stream 274.

Metrics: `{ "destination": "135.148.121.246", "destination\_port": 8080, "duration\_seconds": 55.29, "packets": 19, "source": "172.16.0.149", "wire\_bytes": 2461 }`

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 14063 / TCP stream 281.

Metrics: `{"destination":"168.197.250.14","destination\_port":80,"duration\_seconds":90.205,"packets":19,"source":"172.16.0.170","wire\_bytes":2359}`

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 14528 / TCP stream 293.

Metrics: `{"destination":"168.197.250.14","destination\_port":80,"duration\_seconds":34.782,"packets":21,"source":"172.16.0.170","wire\_bytes":4464}`

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 14623 / TCP stream 298.

Metrics: `{"destination":"168.197.250.14","destination\_port":80,"duration\_seconds":40.858,"packets":201,"source":"172.16.0.170","wire\_bytes":159636}`

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 16159 / TCP stream 306.

Metrics: `{"destination":"162.144.76.184","destination\_port":8080,"duration\_seconds":32.803,"packets":767,"source":"172.16.0.170","wire\_bytes":545561}`

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 17066 / TCP stream 311.

Metrics: `{"destination":"128.199.93.156","destination\_port":8080,"duration\_seconds":36.477,"packets":767,"source":"172.16.0.170","wire\_bytes":546358}`

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 18531 / TCP stream 324.

Metrics: `{"destination":"135.148.121.246","destination\_port":8080,"duration\_seconds":51.515,"packets":422,"source":"172.16.0.149","wire\_bytes":342682}`

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 18949 / TCP stream 325.

Metrics: `{"destination":"135.148.121.246","destination\_port":8080,"duration\_seconds":83.461,"packets":19,"source":"172.16.0.149","wire\_bytes":2922}`

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 19849 / TCP stream 329.

Metrics: `{"destination":"135.148.121.246","destination\_port":8080,"duration\_seconds":35.196,"packets":19,"source":"172.16.0.149","wire\_bytes":2531}`

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 20080 / TCP stream 333.

Metrics: `{"destination":"135.148.121.246","destination\_port":8080,"duration\_seconds":85.095,"packets":19,"source":"172.16.0.149","wire\_bytes":3198}`

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 20948 / TCP stream 367.

Metrics: `{"destination":"139.196.72.155","destination\_port":8080,"duration\_seconds":51.093,"packets":124,"source":"172.16.0.170","wire\_bytes":101936}`

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 21069 / TCP stream 368.

Metrics: `{"destination":"139.196.72.155","destination\_port":8080,"duration\_seconds":38.15,"packets":19,"source":"172.16.0.170","wire\_bytes":3125}`

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 21121 / TCP stream 369.

Metrics: `{"destination":"139.196.72.155","destination\_port":8080,"duration\_seconds":58.283,"packets":413,"source":"172.16.0.170","wire\_bytes":356002}`

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 21759 / TCP stream 390.

Metrics: `{"destination":"185.184.25.78","destination\_port":8080,"duration\_seconds":123.7,"packets":1334,"source":"172.16.0.170","wire\_bytes":1155759}`

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 23259 / TCP stream 411.

Metrics: `{"destination":"54.37.106.167","destination\_port":8080,"duration\_seconds":122.065,"packets":23,"source":"172.16.0.170","wire\_bytes":4023}`

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 23301 / TCP stream 417.

Metrics: `{"destination":"198.199.98.78","destination\_port":8080,"duration\_seconds":95.397,"packets":890,"source":"172.16.0.170","wire\_bytes":789030}`

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 24437 / TCP stream 469.

Metrics: `{"destination":"128.199.192.135","destination\_port":8080,"duration\_seconds":49.124,"packets":302,"source":"172.16.0.170","wire\_bytes":248547}`

ATT&CK candidates

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

Identities

- account: `desktop-kpq9fdb`; client IPs: 172.16.0.149; frames: 1987, 1995, 1997, 2009, 2062
- account: `desktop-vd151o7`; client IPs: 172.16.0.131; frames: 30, 38, 40, 52, 64
- account: `desktop-w5ftqy`; client IPs: 172.16.0.170; frames: 625, 633, 637, 647, 663
- account: `everett.french`; client IPs: 172.16.0.170; frames: 1337, 1345, 1347, 1359, 1373
- account: `nick.montgomery`; client IPs: 172.16.0.149; frames: 2755, 2763, 2765, 2777, 2787
- account: `tricia.becker`; client IPs: 172.16.0.131; frames: 1658, 1666, 1668, 1680, 1699
- domain: `SUNNYSTATION`; client IPs: 172.16.0.131; frames: 1750
- full-name: `Everett French`; client IPs: 172.16.0.170; frames: 1448
- full-name: `Nick Montgomery`; client IPs: 172.16.0.149; frames: 2882
- full-name: `Tricia Becker`; client IPs: 172.16.0.131; frames: 1802
- hostname: `DESKTOP-KPQ9FDB`; client IPs: 172.16.0.149; frames: 1915, 1937, 2040, 2281, 2327
- hostname: `DESKTOP-VD151O7`; client IPs: 172.16.0.131; frames: 1, 10, 99, 293, 361
- hostname: `DESKTOP-W5FTQY`; client IPs: 172.16.0.170; frames: 519, 538, 797, 867, 1074
- netbios-group: `SUNNYSTATION`; client IPs: unbound subject; frames: 11, 292, 389, 393, 397

IOC and artifact candidates

- domain: `a-0010.a-msedge.net`; roles: dns-cname
- domain: `a-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `ajaxmatters.com`; roles: dns-cname
- domain: `api.msn.com`; roles: dns-query, tls-sni
- domain: `autodiscover.sunnystation.com`; roles: dns-query
- domain: `awridahmed.com`; roles: dns-cname
- domain: `b-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `c-ring.msedge.net`; roles: dns-query, tls-sni
- domain: `checkappexec.microsoft.com`; roles: dns-query, tls-sni
- domain: `client.wns.windows.com`; roles: dns-query, tls-sni
- domain: `ctdl.windowsupdate.com`; roles: dns-query, http-host
- domain: `dalgahavuzu.com`; roles: dns-query, tls-sni
- domain: `desktop-kpq9fdb.sunnystation.com`; roles: dns-query
- domain: `desktop-vd151o7.sunnystation.com`; roles: dns-query
- domain: `desktop-w5ftqy.sunnystation.com`; roles: dns-query
- domain: `dns.msftncsi.com`; roles: dns-query
- domain: `ecs.office.com`; roles: dns-query, tls-sni
- domain: `ext-cust.squarespace.com`; roles: dns-cname
- domain: `fe2cr.update.microsoft.com`; roles: dns-query, tls-sni

- domain: `fe2cr.update.msft.com.trafficmanager.net`; roles: dns-cname
- domain: `fe3cr.delivery.mp.microsoft.com`; roles: dns-query, tls-sni
- domain: `fp-afd-nocache.azureedge.net`; roles: dns-query, tls-sni
- domain: `fp-afd.azureedge.us`; roles: dns-query, tls-sni
- domain: `fp-afd.azurefd.us`; roles: dns-query, tls-sni
- domain: `fp-as-nocache.azureedge.net`; roles: dns-query, tls-sni
- domain: `fp-as.azureedge.net`; roles: dns-query, tls-sni
- domain: `fp-vp.azureedge.net`; roles: dns-query, tls-sni
- domain: `fs.microsoft.com`; roles: dns-query, tls-sni
- domain: `gator4020.hostgator.com`; roles: dns-query
- domain: `ghs.googlehosted.com`; roles: dns-cname
- domain: `globalsovereignbank.com`; roles: dns-cname
- domain: `imap.123-reg.co.uk`; roles: dns-query
- domain: `imap.aol.com`; roles: dns-query
- domain: `imap.gmail.com`; roles: dns-query
- domain: `imap.ionos.mx`; roles: dns-query
- domain: `imap.secureserver.net`; roles: dns-query
- domain: `internal-aol.imap.mail.g03.yahoodns.net`; roles: dns-cname
- domain: `ipv6.msftncsi.com`; roles: dns-query
- domain: `isatap.localdomain`; roles: dns-query
- domain: `isatap.sunnystation.com`; roles: dns-query
- domain: `login.live.com`; roles: dns-query, tls-sni
- domain: `login.microsoftonline.com`; roles: dns-query, tls-sni
- domain: `mail.alienergy.com.pk`; roles: dns-query
- domain: `mail.gmail.com`; roles: dns-query
- domain: `mail.idn-ltd.com`; roles: dns-query
- domain: `mail.ionos.com`; roles: dns-query
- domain: `mail.mail.com`; roles: dns-query
- domain: `mail.mail.yahoo.com`; roles: dns-query
- domain: `mail.mitsuwagroup.co.jp`; roles: dns-query
- domain: `mail.proteinchile.cl`; roles: dns-query
- domain: `mail.sapporo-kiden.co.jp`; roles: dns-query
- domain: `mail.zoho.com`; roles: dns-query
- domain: `mitsuwagroup.co.jp`; roles: dns-cname
- domain: `nexusrules.officeapps.live.com`; roles: dns-query, tls-sni
- domain: `odc.officeapps.live.com`; roles: dns-query, tls-sni
- domain: `ow1.res.office365.com`; roles: dns-query, tls-sni
- domain: `parkingpage.namecheap.com`; roles: dns-cname
- domain: `pop.km-plan.co.jp`; roles: dns-query
- domain: `privilegetroissecurity.com`; roles: dns-cname
- domain: `prod.nexusrules.live.com.akadns.net`; roles: dns-cname
- domain: `proteinchile.cl`; roles: dns-cname
- domain: `pti.store.microsoft.com`; roles: dns-query, tls-sni
- domain: `riskprotek.com`; roles: dns-cname
- domain: `s-ring.msedge.net`; 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: `shops.myshopify.com`; roles: dns-cname
- domain: `smtp.aruba.it`; roles: dns-query
- domain: `smtp.bstem.jp`; roles: dns-query
- domain: `smtp.hanwa-net.co.jp`; roles: dns-query
- domain: `smtp.live.com`; roles: dns-query
- domain: `smtp.mail.com`; roles: dns-query
- domain: `smtp.nifty.com`; roles: dns-query
- domain: `smtp.ocn.ne.jp`; roles: dns-query
- domain: `smtp.office365.com`; roles: dns-query
- domain: `smtp.secureserver.net`; roles: dns-query
- domain: `sunnyfileservers.sunnystation.com`; roles: dns-query
- domain: `sunnystation-dc.sunnystation.com`; roles: dns-query
- domain: `sunnystation.com`; roles: dns-query
- domain: `target.clickfunnels.com`; roles: dns-cname
- domain: `tring.clo.footprintdns.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: `wns.notify.trafficmanager.net`; roles: dns-cname

- domain: `wpad.localdomain`; roles: dns-query
- domain: `wpad.sunnystation.com`; roles: dns-query
- domain: `www.32342240.xyz`; roles: dns-query
- domain: `www.ajaxmatters.com`; roles: dns-query, http-host
- domain: `www.awridahmed.com`; roles: dns-query, http-host
- domain: `www.ban-click.com`; roles: dns-query, http-host
- domain: `www.barrcoplumbingsupply.com`; roles: dns-query
- domain: `www.bing.com`; roles: dns-query, tls-sni
- domain: `www.byaliciafryearson.com`; roles: dns-query
- domain: `www.campdiscount.info`; roles: dns-query, http-host
- domain: `www.centroimprenta.xyz`; roles: dns-query
- domain: `www.chinadqwx.com`; roles: dns-query, http-host
- domain: `www.czzhudi.com`; roles: dns-query, http-host
- domain: `www.db-propertygroup.com`; roles: dns-query, http-host
- domain: `www.e-scooters.frl`; roles: dns-query
- domain: `www.elsiepupz.com`; roles: dns-query, http-host
- domain: `www.freedomteaminc.com`; roles: dns-query
- domain: `www.globalsovereignbank.com`; roles: dns-query, http-host
- domain: `www.hentainftxxx.com`; roles: dns-query, http-host
- domain: `www.hydrocheats.com`; roles: dns-query, http-host
- domain: `www.jmtmjz.com`; roles: dns-query
- domain: `www.jogoreviravolta.com`; roles: dns-query, http-host
- domain: `www.katchybugonsale.com`; roles: dns-query, http-host
- domain: `www.keysine.com`; roles: dns-query, http-host
- domain: `www.klassociates.info`; roles: dns-query
- domain: `www.krpano.pro`; roles: dns-query
- domain: `www.moonshot.properties`; roles: dns-query, http-host
- domain: `www.msftncsi.com`; roles: dns-query, http-host
- domain: `www.mystore.guide`; roles: dns-query, http-host
- domain: `www.nt-renewable.com`; roles: dns-query, http-host
- domain: `www.privilegetroissecurity.com`; roles: dns-query, http-host
- domain: `www.riskprotek.com`; roles: dns-query, http-host
- domain: `www.seo-python.com`; roles: dns-query, http-host
- domain: `www.theperfecttrainer.com`; roles: dns-query, http-host
- domain: `www.xn--pckwb0cye6947ajzku8opzi.com`; roles: dns-query, http-host
- domain: `yahoo.com`; roles: dns-query
- ipv4: `0.0.0.0`; roles: network-endpoint
- ipv4: `103.41.204.169`; roles: network-endpoint
- ipv4: `103.42.57.17`; roles: network-endpoint
- ipv4: `104.131.62.48`; roles: network-endpoint
- ipv4: `104.16.12.194`; roles: dns-answer, network-endpoint
- ipv4: `104.16.13.194`; roles: dns-answer
- ipv4: `104.16.14.194`; roles: dns-answer
- ipv4: `104.16.15.194`; roles: dns-answer
- ipv4: `104.16.16.194`; roles: dns-answer
- ipv4: `104.21.89.147`; roles: dns-answer, network-endpoint
- ipv4: `104.212.67.52`; roles: dns-answer, network-endpoint
- ipv4: `104.212.67.71`; roles: dns-answer, network-endpoint
- ipv4: `116.254.112.253`; roles: dns-answer, network-endpoint
- ipv4: `118.98.72.86`; roles: network-endpoint
- ipv4: `120.55.51.124`; roles: dns-answer, network-endpoint
- ipv4: `122.17.147.238`; roles: dns-answer, network-endpoint
- ipv4: `128.199.192.135`; roles: network-endpoint
- ipv4: `128.199.93.156`; roles: network-endpoint
- ipv4: `13.107.21.200`; roles: dns-answer, network-endpoint
- ipv4: `13.107.213.57`; roles: dns-answer
- ipv4: `13.107.246.254`; roles: dns-answer, network-endpoint
- ipv4: `13.107.246.57`; roles: dns-answer, network-endpoint
- ipv4: `13.107.3.254`; roles: dns-answer, network-endpoint
- ipv4: `13.107.4.254`; roles: dns-answer, network-endpoint
- ipv4: `13.107.6.254`; roles: dns-answer, network-endpoint
- ipv4: `13.89.178.27`; roles: dns-answer, network-endpoint
- ipv4: `131.107.255.255`; roles: dns-answer
- ipv4: `134.209.156.68`; roles: network-endpoint
- ipv4: `135.148.121.246`; roles: network-endpoint

- ipv4: `136.143.191.104`; roles: dns-answer, network-endpoint
- ipv4: `139.196.72.155`; roles: network-endpoint
- ipv4: `142.250.138.108`; roles: dns-answer
- ipv4: `142.250.138.109`; roles: dns-answer, network-endpoint
- ipv4: `144.217.88.125`; roles: network-endpoint
- ipv4: `154.206.65.249`; roles: dns-answer, network-endpoint
- ipv4: `156.96.154.210`; roles: http-host, network-endpoint
- ipv4: `159.69.237.188`; roles: network-endpoint
- ipv4: `162.144.76.184`; roles: network-endpoint
- ipv4: `168.197.250.14`; roles: network-endpoint
- ipv4: `172.16.0.1`; roles: network-endpoint
- ipv4: `172.16.0.131`; roles: dns-answer, network-endpoint
- ipv4: `172.16.0.149`; roles: dns-answer, network-endpoint
- ipv4: `172.16.0.170`; roles: dns-answer, network-endpoint
- ipv4: `172.16.0.255`; roles: network-endpoint
- ipv4: `172.16.0.52`; roles: dns-answer, network-endpoint
- ipv4: `172.16.0.53`; roles: dns-answer, network-endpoint
- ipv4: `172.67.160.224`; roles: dns-answer
- ipv4: `173.201.192.129`; roles: dns-answer
- ipv4: `173.201.192.158`; roles: dns-answer
- ipv4: `173.201.193.240`; roles: dns-answer, network-endpoint
- ipv4: `173.201.193.97`; roles: dns-answer
- ipv4: `173.231.37.114`; roles: dns-answer, network-endpoint
- ipv4: `178.211.56.194`; roles: dns-answer, network-endpoint
- ipv4: `180.250.21.2`; roles: network-endpoint
- ipv4: `184.168.99.26`; roles: dns-answer, network-endpoint
- ipv4: `185.148.168.15`; roles: network-endpoint
- ipv4: `185.148.168.220`; roles: network-endpoint
- ipv4: `185.184.25.78`; roles: network-endpoint
- ipv4: `190.90.233.66`; roles: network-endpoint
- ipv4: `191.252.103.16`; roles: network-endpoint
- ipv4: `192.185.4.31`; roles: dns-answer, network-endpoint
- ipv4: `194.9.172.107`; roles: network-endpoint
- ipv4: `194.9.94.85`; roles: dns-answer, network-endpoint
- ipv4: `194.9.94.86`; roles: dns-answer
- ipv4: `195.154.146.35`; roles: network-endpoint
- ipv4: `198.185.159.144`; roles: dns-answer, network-endpoint
- ipv4: `198.185.159.145`; roles: dns-answer
- ipv4: `198.199.98.78`; roles: network-endpoint
- ipv4: `198.49.23.144`; roles: dns-answer
- ipv4: `198.49.23.145`; roles: dns-answer
- ipv4: `198.54.117.210`; roles: dns-answer, network-endpoint
- ipv4: `198.54.117.211`; roles: dns-answer
- ipv4: `198.54.117.212`; roles: dns-answer
- ipv4: `198.54.117.215`; roles: dns-answer, network-endpoint
- ipv4: `198.54.117.216`; roles: dns-answer
- ipv4: `198.54.117.217`; roles: dns-answer
- ipv4: `198.54.117.218`; roles: dns-answer
- ipv4: `20.140.147.202`; roles: dns-answer, network-endpoint
- ipv4: `20.189.173.11`; roles: dns-answer, network-endpoint
- ipv4: `20.189.173.15`; roles: dns-answer, network-endpoint
- ipv4: `20.189.173.3`; roles: dns-answer, network-endpoint
- ipv4: `20.189.173.9`; roles: dns-answer, network-endpoint
- ipv4: `20.190.157.11`; roles: dns-answer
- ipv4: `20.42.73.24`; roles: dns-answer, network-endpoint
- ipv4: `20.42.73.25`; roles: dns-answer, network-endpoint
- ipv4: `20.44.10.122`; 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: `204.79.197.212`; roles: dns-answer, network-endpoint
- ipv4: `204.79.197.254`; roles: dns-answer, network-endpoint
- ipv4: `209.17.116.163`; roles: dns-answer, network-endpoint
- ipv4: `210.131.2.36`; roles: dns-answer, network-endpoint

- ipv4: `210.57.209.142`; roles: network-endpoint
- ipv4: `211.13.204.5`; roles: dns-answer, network-endpoint
- ipv4: `211.16.12.137`; roles: dns-answer, network-endpoint
- ipv4: `213.186.33.5`; roles: dns-answer, network-endpoint
- ipv4: `216.172.184.77`; roles: dns-answer, network-endpoint
- ipv4: `216.230.252.20`; roles: dns-answer, network-endpoint
- ipv4: `216.58.193.147`; 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: `23.218.224.137`; roles: dns-answer, network-endpoint
- ipv4: `23.218.224.148`; roles: dns-answer
- ipv4: `23.218.224.151`; roles: dns-answer, network-endpoint
- ipv4: `23.218.224.154`; roles: dns-answer, network-endpoint
- ipv4: `23.227.38.74`; roles: dns-answer, network-endpoint
- ipv4: `23.29.115.34`; roles: dns-answer, network-endpoint
- ipv4: `23.38.92.72`; roles: dns-answer, network-endpoint
- ipv4: `23.47.49.133`; roles: dns-answer, network-endpoint
- ipv4: `23.47.49.165`; roles: dns-answer, network-endpoint
- ipv4: `239.255.255.250`; roles: http-host, network-endpoint
- ipv4: `255.255.255.255`; roles: network-endpoint
- ipv4: `27.254.174.84`; roles: network-endpoint
- ipv4: `27.34.147.95`; roles: dns-answer, network-endpoint
- ipv4: `3.130.204.160`; roles: dns-answer
- ipv4: `3.130.253.23`; roles: dns-answer, network-endpoint
- ipv4: `37.44.244.177`; roles: network-endpoint
- ipv4: `37.59.209.141`; roles: network-endpoint
- ipv4: `40.125.122.151`; roles: dns-answer, network-endpoint
- ipv4: `40.126.28.11`; roles: dns-answer
- ipv4: `40.126.28.12`; roles: dns-answer
- ipv4: `40.126.28.13`; roles: dns-answer, network-endpoint
- ipv4: `40.126.28.14`; roles: dns-answer
- ipv4: `40.126.28.18`; roles: dns-answer
- ipv4: `40.126.28.19`; roles: dns-answer, network-endpoint
- ipv4: `40.126.28.20`; roles: dns-answer
- ipv4: `40.126.28.21`; roles: dns-answer
- ipv4: `40.126.28.22`; roles: dns-answer
- ipv4: `40.126.28.23`; roles: dns-answer
- ipv4: `40.126.29.10`; roles: dns-answer
- ipv4: `40.126.29.11`; roles: dns-answer
- ipv4: `40.126.29.12`; roles: dns-answer
- ipv4: `40.126.29.13`; roles: dns-answer
- ipv4: `40.126.29.15`; roles: dns-answer
- ipv4: `40.126.29.5`; roles: dns-answer
- ipv4: `40.126.29.6`; roles: dns-answer, network-endpoint
- ipv4: `40.126.29.7`; roles: dns-answer
- ipv4: `40.126.29.8`; roles: dns-answer
- ipv4: `40.126.29.9`; roles: dns-answer, network-endpoint
- ipv4: `40.126.7.32`; roles: dns-answer, network-endpoint
- ipv4: `40.126.7.35`; roles: dns-answer, network-endpoint
- ipv4: `40.83.240.146`; roles: dns-answer, network-endpoint
- ipv4: `40.97.120.162`; roles: dns-answer, network-endpoint
- ipv4: `40.97.199.114`; roles: dns-answer
- ipv4: `45.71.195.104`; roles: network-endpoint
- ipv4: `52.109.20.76`; roles: dns-answer, network-endpoint
- ipv4: `52.109.76.31`; 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: `52.113.194.132`; roles: dns-answer, network-endpoint
- ipv4: `52.168.117.169`; roles: dns-answer, network-endpoint
- ipv4: `52.182.141.63`; 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: `52.238.248.0`; roles: dns-answer
- ipv4: `52.238.248.1`; roles: dns-answer, network-endpoint

- ipv4: `52.238.248.4`; roles: dns-answer, network-endpoint
- ipv4: `52.96.122.242`; roles: dns-answer
- ipv4: `52.96.191.98`; roles: dns-answer
- ipv4: `54.37.106.167`; roles: network-endpoint
- ipv4: `54.37.228.122`; roles: network-endpoint
- ipv4: `54.38.242.185`; roles: network-endpoint
- ipv4: `59.148.253.194`; roles: network-endpoint
- ipv4: `61.7.231.226`; roles: network-endpoint
- ipv4: `61.7.231.229`; roles: network-endpoint
- ipv4: `64.34.171.228`; roles: dns-answer, network-endpoint
- ipv4: `65.52.5.117`; roles: dns-answer, network-endpoint
- ipv4: `66.218.86.51`; roles: dns-answer, network-endpoint
- ipv4: `66.235.200.112`; roles: dns-answer, network-endpoint
- ipv4: `66.29.145.216`; roles: dns-answer, network-endpoint
- ipv4: `68.178.213.203`; roles: dns-answer, network-endpoint
- ipv4: `68.178.213.37`; roles: dns-answer
- ipv4: `68.178.252.117`; roles: dns-answer
- ipv4: `68.183.93.250`; roles: network-endpoint
- ipv4: `72.167.191.69`; roles: dns-answer, network-endpoint
- ipv4: `72.167.218.138`; roles: dns-answer
- ipv4: `72.167.238.29`; roles: dns-answer
- ipv4: `72.21.81.200`; roles: dns-answer, network-endpoint
- ipv4: `74.208.255.201`; roles: dns-answer, network-endpoint
- ipv4: `74.208.5.10`; roles: dns-answer, network-endpoint
- ipv4: `74.208.5.15`; roles: dns-answer, network-endpoint
- ipv4: `74.6.141.28`; roles: dns-answer
- ipv4: `74.6.143.25`; roles: dns-answer
- ipv4: `74.6.143.26`; roles: dns-answer
- ipv4: `74.6.229.28`; roles: dns-answer
- ipv4: `74.6.231.20`; roles: dns-answer, network-endpoint
- ipv4: `74.6.231.21`; roles: dns-answer
- ipv4: `78.46.73.125`; roles: network-endpoint
- ipv4: `85.214.67.203`; roles: network-endpoint
- ipv4: `94.136.40.232`; roles: dns-answer, network-endpoint
- ipv4: `94.177.209.30`; roles: dns-answer, network-endpoint
- ipv4: `96.7.168.59`; roles: dns-answer, network-endpoint
- ipv4: `97.74.135.10`; roles: dns-answer
- ipv4: `97.74.135.143`; roles: dns-answer
- ipv4: `98.137.11.163`; roles: dns-answer
- ipv4: `98.137.11.164`; roles: dns-answer
- ipv4: `98.137.159.60`; roles: dns-answer
- ja3: `28a2c9bd18a11de089ef85a160da29e4`; roles: tls-client-fingerprint
- ja3: `37cdab6ff1bd1c195bacb776c5213bf2`; roles: tls-client-fingerprint
- ja3: `37f463bf4616ecd445d4a1937da06e19`; roles: tls-client-fingerprint
- ja3: `3b5074b1b5d032e5620f69f9f700ff0e`; roles: tls-client-fingerprint
- ja3: `51c64c77e60f3980eeaa90869b68c58a8`; roles: tls-client-fingerprint
- ja3: `6271f898ce5be7dd52b0fc260d0662b3`; roles: tls-client-fingerprint
- ja3: `a0e9f5d64349fb13191bc781f81f42e1`; roles: tls-client-fingerprint
- sha256: `004599278fd2775eb468eac406e47dab4e5775c32eeb98a0f7ff21768aa2fdcf`; roles: exported-object
- sha256: `0119adca455bfe449a3b6d30660b9a4fb4d7f9b1a42504166debb61bc7a1a64`; roles: exported-object
- sha256: `012525bd08b8856409471857cddde9928f6f5505e0eedfdc05880783621712242`; roles: exported-object
- sha256: `02751d70749d493ba1989b74765a1cd1c56294db42c8b7775b3c0172828df4a6`; roles: exported-object
- sha256: `03e81cfa927c6cdce33587023c24bb89f21cf506458598c7624bc61c8d3f8e58`; roles: exported-object
- sha256: `0417dd954d3695d2bf400f237806c505bf8ccccf07c44ce9467d98ed4175ea255`; roles: exported-object
- sha256: `04b3ca7f09694f7f1b8e7b71f3503d325b75d3ff938ed24eeb9939714635f0d2`; roles: exported-object
- sha256: `04b4f6035a50b1f58ebddb3f5a3e8cf1949a9b6b36b497c86b2b8c2b91e7ad4f`; roles: exported-object
- sha256: `04ded8bd35a45a9dd083f3cc32056559c2d62739e5edebdaf1be2b5bf6133ea3`; roles: exported-object
- sha256: `051f4c30c5306ffeff3f92010446f0aa0c420978da429cb787c50604c5944174`; roles: exported-object
- sha256: `05497fa07eb6f2ee015c09ace90d0423c20136b9c6e4a52ee3e4c60c376eac3`; roles: exported-object
- sha256: `05b0dc4e3b3623d8fe2e6d653af5f42f73ce33b8d5461de62b0b113aa5f3caa0`; roles: exported-object
- sha256: `05ba7c0984a69934dba3a41191243d8dc8fd5abf2fea86a4ead813cf2a9d9dee`; roles: exported-object
- sha256: `05dfb38ed78ba413e07d3e01d40dd139683aa9b4715d3f000abc9d95e16205a6`; roles: exported-object
- sha256: `0604cda2873562b6894fce5ef33aab23eeb01abae54bfd1a3ade48e85e54f266`; roles: exported-object
- sha256: `0609a4da54220690f415ac4d27cee84f2eea7d6a39ae990017ac25889ca2ca54`; roles: exported-object
- sha256: `06af7d2c9ddd3737f67c6789e4fa2610ed99d3d4aeb157e15c9f0b3eab46ceed`; roles: exported-object

- sha256: `08387b61ba8264eef8f26f5d669b04b28b0ae71ee8ffe4de6852c8c2b9668d3d`; roles: exported-object
- sha256: `08ff66f98bdcf6573485fb6a07e45b72de258edb90706aa75260b1f541a961eb`; roles: exported-object
- sha256: `0965a8861f7f70048f6251a520c65bf2930b3b9265e0e55142aa384f4da36f24`; roles: exported-object
- sha256: `09b156788ec22bd98b36d95565ab19199d442dc653c73ddbabb3525792130b593`; roles: exported-object
- sha256: `09ba1e573a77d25cfe065aa002a155189ce4f5cbfb0251ab61dc3b5eea9569f5`; roles: exported-object
- sha256: `0a1b9616d1191c67cb63f7b1b8bd9809f43c94a183eb23527df28490ac9666f7`; roles: exported-object
- sha256: `0aa09ec450e32afa62a72eeb252e83ad291b68ed378fb455ee4cb618ba04849a`; roles: exported-object
- sha256: `0b0e4ae56a34d0aa05dca4d67700c3964c649f66bc9d9afd2c430bdb1f063be8`; roles: exported-object
- sha256: `0b500a7b1a98e79df9f948812495251061d45e48ee19eb795810272216b6fbc9`; roles: exported-object
- sha256: `0bd44562868ac54cb8c1043310b8f1d8267e681908bbd1d5e14b27ce796b977d`; roles: exported-object
- sha256: `0ded265abee66125302a95e54828bf136e471f93d1c6ddbaec3513f4960254b6`; roles: exported-object
- sha256: `0df6c8212c4a7361f440ffbd1ee76222cbc3d4e24b3c2716946800e13fd8ce8`; roles: exported-object
- sha256: `0e60578c595f5d1d852562e954c270edcaec54de126892ebf8dc2a60c9b1503`; roles: exported-object
- sha256: `0ec2306524e6c599765d5d1223e9a33329d8c0793039e8d26c15de173d79e958`; roles: exported-object
- sha256: `0f102e9552d90e78af23de4a7b4411569878a3149aaebc38e5168e422c5d247e`; roles: exported-object
- sha256: `0f99ac235c51cdf782c4f8193f4698892a38d6365845031d7b20f976196fe4f`; roles: exported-object
- sha256: `0ff8e752caa95643bf7b3776d821737814f87fe3d6925701a3183971391edcf`; roles: exported-object
- sha256: `0ffbddc5bc92b9e3b50893241fa9a182f02ab2a61054568668bec4f2e8a08fe9`; roles: exported-object
- sha256: `10570ef48a963eeab20a1bd339618b44d213b436c19c51fb05099183a9999f4b`; roles: exported-object
- sha256: `10e9248a956dcfbdb1d4c8b70dd05ee54605208b614d10ceb7b8b88d150cb0ef`; roles: exported-object
- sha256: `118a94f5308fb6dd5bf0096ef766eb9fdc207a1c05fc23c7186aba49100ee508`; roles: exported-object
- sha256: `120f7dd788fe12ca8c9af5f9d47d1fa963b0f63bc63cef3afcd28ab66bdbbf6f`; roles: exported-object
- sha256: `121098e0cde0a928173ac2ba2da6dd82b1b626453b296059c60926787b1e4546`; roles: exported-object
- sha256: `1235888074ede34f478e3108c85f05795ab16d8fb72b534547fb0da3e6a234e`; roles: exported-object
- sha256: `129c768192359093317c1b658b106ba3d9968476a695fef49ea9e6d118467767`; roles: exported-object
- sha256: `139f6fa785927256480056be4662ba4122fa4e5a18d7b63752f8d2ae6c9395b6`; roles: exported-object
- sha256: `13bf0aa04849e77d7914f426c28a54bb49f547cc004ae800af68864980a4a88d`; roles: exported-object
- sha256: `14245b645e4103d8713e7f916fc7d4d10ae98146a05af38d2b800d52c8acc717`; roles: exported-object
- sha256: `142855918acb873018e7afb636a8f9d0495b3028b4d16b4cf706d68b3a7f8ce3`; roles: exported-object
- sha256: `147f4226dc3c57cb9d2536c745013d7145af769c26fc6b37d0848a01af884865`; roles: exported-object
- sha256: `148dd3a46202949f4ff34c20da8804f68644abec319cbfd57efb774b9b3ebf5d`; roles: exported-object
- sha256: `14a5cc536d16a41573e57bfe68ede705cb5850500eaa5ec123c42784903055c0`; roles: exported-object
- sha256: `14b57211308ac8ad2a63c965783d9ba1c2d1930d0cafd884374d143a481f9bf3`; roles: exported-object
- sha256: `14c39252741654b6e9872383aa869070317abb18e91fd5d8bb1341b3abe62c4`; roles: exported-object
- sha256: `14cd9376ff8f1a914c40168783efb3d4e8f53c2526378000a0190478621eac9f`; roles: exported-object
- sha256: `157889eb6bfcd5fb11eca24228c4f9ae1a176455785456ca79849fb0bb5c2792`; roles: exported-object
- sha256: `15861b469b40931e7dbe3a8b6aacb1ee6824b431fea25281840e1db28086d255`; roles: exported-object
- sha256: `161004698346c45313eef873dc3e555f83bf5f4fd616d1f67947fbc8cf3b2660`; roles: exported-object
- sha256: `1694f0ee7be6029fe279792606f74d0e0c156eedf216eb6d30753048e33ac95c`; roles: exported-object
- sha256: `16f02f7a9a59c59bf6b7651c334043da2c43d100661c8345dce857c8743374b0`; roles: exported-object
- sha256: `178252c182d98d603e7235df45e57e1d92aa93fc0c3b71d5c27bc1b7b1c7c310`; roles: exported-object
- sha256: `178ca47275e40b28d97e3f2445c90926cecad89d7679ee5eb59cd1917041f61e`; roles: exported-object
- sha256: `18ce8668476bb27422129b0f9e3992cafb555779513b7c73daa5e1b07577dbf1`; roles: exported-object
- sha256: `191a086e159061a0c87247adcfe042e6c15854fca15397fe2dc99a0f35efa1ed`; roles: exported-object
- sha256: `195aaab78e060cb793d406f91c91592c44a15d944ae7662a5fd8dc7750a121dd`; roles: exported-object
- sha256: `1970d832434fda01eee7325d7882f19089ff3dc6b6e623be0e2be3e21da60290`; roles: exported-object
- sha256: `199efb2dba801fbe4f06b60162b3cc083a63d6078f6b56224f5dc538ded3bdf4`; roles: exported-object
- sha256: `1a188e05405f1ce01789dc73de2d60632eade6ad95f36cec29b988444861eb1`; roles: exported-object
- sha256: `1a281a2d280c6d1f1f205d3f8210057b1b555794f6c12db57e4e8e4816cb9036`; roles: exported-object
- sha256: `1bc147f6a38ee4f00397689ae7cbaae2a9807b40d09092404c90dbe97611ab079`; roles: exported-object
- sha256: `1bc0c79371604a7e57f527a518397cbbfc312314c6213ac27b44d3a62abd87f17`; roles: exported-object
- sha256: `1c19ebc675280676ea53db434f16e8f1b97b729785511d5c82ebb610fb53f08d`; roles: exported-object
- sha256: `1c3694a1647d000fce54a9d5a30c1a06da57a9e6fab75870993b4d5653577417`; roles: exported-object
- sha256: `1cd3bcdffa4cebaeba570316c23a0248dfb1dd90898bca8e1bf01596b5beedcc`; roles: exported-object
- sha256: `1d16bd195b28177d0030375134b90eab863a25458c56d05c7e72ecfcd8ddfb8`; roles: exported-object
- sha256: `1d21900f027764a25c787c4e444214277ab36e2074037e5d5a8ce6f0efbb004e`; roles: exported-object
- sha256: `1d71eef40b1c844cb461ecc7197ed8eef6bc582ba1e5dc287c3bf5fc15e1b4af`; roles: exported-object
- sha256: `1db156538dd79f08b09c654f86b8f6d481d588fa44cc51f02c4e42fcdca7913`; roles: exported-object
- sha256: `1de41672c3a500d7321663f486920a8fb5f29e8801f92be3e1aa60cb78bddbf7`; roles: exported-object
- sha256: `1f0fd84ce2a8a3ae572963ae3ad0937920664b081fe79acf87fde2b13acc77be`; roles: exported-object
- sha256: `1f68d99e75eadd0dbd08ee26e222e4a21040c56a6266f1d0d9b385730ca12fc0`; roles: exported-object
- sha256: `1fe5730bb3502850c53ca50dc874702126977f857a47c3dbe5d1a1226afd5c08`; roles: exported-object
- sha256: `206abeeabef598ad3c984ba9e8b3d56d663989b35c5074ef330514b5841e1a6e`; roles: exported-object
- sha256: `209565664129ec0b9c01867286aa093f1ca15e4ad12093aac53bc290925ae39f`; roles: exported-object
- sha256: `211aa041d8b4ea3a643d44eb8f538f6caa0a5e0e3b63a802de3fbf0a9011a1f1`; roles: exported-object

- sha256: `2143e3b14753fe28b4e495e57c087ef8fea10cbd644761105d607d90b9d23633`; roles: exported-object
- sha256: `2194c3bdb83d8e73218ec1fc36977bd7566500eb0cc264750ce08248f7575543`; roles: exported-object
- sha256: `21abcfcccc584af261252953ef89fd36141f086a365fbd9d2066ae94b3c4bd76`; roles: exported-object
- sha256: `2251efee138848fe36171baae0d12828489e0bcc3b063bc509e2724cf671c01f`; roles: exported-object
- sha256: `2269981a9b387528f38aaa58c273b3a203ba1ce1e4ab7d369210e411cedaef46`; roles: exported-object
- sha256: `22704106a20c5a5a5f4c78a113092eade0f683945a2496a9a0d5bc69c52bd814`; roles: exported-object
- sha256: `2321ba015f0e7a3d74e190c407ecc25f0b772956eb0645036818a324965264ee`; roles: exported-object
- sha256: `2330b96b60d76e24f5bfcc6d9a4e415cb57d4a8c18d95d50566701d112ab2ca9`; roles: exported-object
- sha256: `23f00aaf4245b4855825f38da30d464bef3c6f81eea7235c99fc7bd5d6b726a3`; roles: exported-object
- sha256: `23f6e432c83a9a3dcb731391e864afb6129df0a7eedda745e7cc51baf1ea1ad2`; roles: exported-object
- sha256: `248430bf42f12f2b4e703bb156543d496f2890ad08148d590f93348830c1ad52`; roles: exported-object
- sha256: `24ec4098e828c89dfb5810b1e4df67cd3e8987e672b16a393e1045ba3ded185e`; roles: exported-object
- sha256: `24feb82784833ef28e43907591d6823fb703d92e6a3960435bea7934a35f15e1`; roles: exported-object
- sha256: `253dd1918125d171a4877950898de2ca26060c40b1d05c8fe31cc9fb56776472`; roles: exported-object
- sha256: `25911c516fcaaded9ea55ede4e30828fe8e21e9a895f5e8948034e9621343854`; roles: exported-object
- sha256: `2620bf96201e9f328aee98a74ce5b87f221e761a8b2662974b35f90991404337`; roles: exported-object
- sha256: `263bc7831746b36b6903d8f193117e6f1e777b2e8765086740b8c0b2af19630e`; roles: exported-object
- sha256: `26d630a69965af7110e23e7d89e870aa432f466b8e25d825ba90a1d615b74765`; roles: exported-object
- sha256: `2741234de895bed810734f6b55872a58fc208957ab25ecea14b7aed45f7c5726`; roles: exported-object
- sha256: `274e7318a4440240d24701135a3a037ffc4064ab6e18b7683968d7ad7557823c`; roles: exported-object
- sha256: `2756bae8f350efe025c1a19b8c04b741660f265fa60d9accbdcee7575d65a301`; roles: exported-object
- sha256: `276fdf588903250404f05a86da40c2e5c26360c7dd2cfce409d8eaf30640e1e6`; roles: exported-object
- sha256: `28204d9f1d7b8c17b7cd049bf7f32b5dc41e538ad9c17d884c1e06eab2d8dd39`; roles: exported-object
- sha256: `28c04e7c2529f941c2276321566ed73a1cd75404e1b419a0ed1afe2ef1e4bb5c`; roles: exported-object
- sha256: `29804a73896b8364000f4c23c69de02f4b4305e30f21c39a39097ac982863ee8`; roles: exported-object
- sha256: `29a06c4b40fada661ba0e4f26673529c42d9bd1fffb629bfd06cdea351634ae`; roles: exported-object
- sha256: `29b84a0556ab8203d2e5fde7529491a0253e9586cf9506583cf50acf715f08cc`; roles: exported-object
- sha256: `29bce0e3976c1a4b0c5a3dedaf4c1df15560fed60eefc170b4e8f1bfd72e881e`; roles: exported-object
- sha256: `2a223bc66bee6f01307afacca8cd03c762c109e39095bf5329d7d70920cdf601`; roles: exported-object
- sha256: `2b785b0137066ea6c9bcb8baa757e5633539962796080eeb05ccd3d775f40845`; roles: exported-object
- sha256: `2b79250e166209b04e6221f70295861958a9388503c781ddd638cc3864843f5a`; roles: exported-object
- sha256: `2b999f47b936dc400728793101b43657b4e9410a7267fb92cd15fac90fd2a482`; roles: exported-object
- sha256: `2ba817fc45bb0dec23acca80833f3e7d19a99b3fc71f3e2fa673ef4c38cf533c`; roles: exported-object
- sha256: `2c1b8be8a085bd2d29dc9c0fde032117a77193ad438602390554138f7cdf4cf`; roles: exported-object
- sha256: `2cc04e0598d2938235c3ef5eeca39c65285f0dcb3149c70fc0a7362a4ea3f490`; roles: exported-object
- sha256: `2d3a83cf33a1a7bbe0b8d0d003e520924b0aa95732828cc17290fb9d461ab96b`; roles: exported-object
- sha256: `2d4829a665a6465d8a67a009389b86e8068c01ce3d094f0459de4ed5f4ef2199`; roles: exported-object
- sha256: `2d4c01d66de1641649052c860fd1a8788f5193fdb96487f4f2d6d82a35d6d07`; roles: exported-object
- sha256: `2de61824c9fcd4a84764dee59289619829a98149225fc246989abf4dfcd5913a`; roles: exported-object
- sha256: `2df0449ed47af847f3b17afa4cdfb3ed4b11a0df006bc7b090fe4f4f74b59f`; roles: exported-object
- sha256: `2e24ef287ea02c7f4c4cc2826389e7b69d3d559d35adbcbdc9b3d7437bd772f5`; roles: exported-object
- sha256: `2e3c453bd6dbe6301f70359c32ff7b03f3c6599208e18fec224196b77ae633d`; roles: exported-object
- sha256: `2ef86698bfc9c4ce9dacd4733967d03b4b58e2130c0905f1ae479e689c767234`; roles: exported-object
- sha256: `2f41a6bbfe2c57b767df989d53cad14278bcaa7b0fe886f8c6b1e7f0cab3c019`; roles: exported-object
- sha256: `2f6d5d053ebbfcb3abd90f94bc862175c2782dd5cc60fb9dbb82a2fe9e8ebaf2`; roles: exported-object
- sha256: `311456b3d2193c6a82531c7338dba44beae1363a17ecfcaee9ead85549f3f666`; roles: exported-object
- sha256: `311b06d1311f38632a53291a497a27877e1d9bed83ed7d344fb3110938ceb1fa`; roles: exported-object
- sha256: `313ac03b87cec74ab7068a0c183daed376e45377fa754059eb752e64fa5c5186`; roles: exported-object
- sha256: `31b2c11ae258a1e49a65bfc346e74b260221370dcd5ccf9f3761399de9f71b3d`; roles: exported-object
- sha256: `31f63b033376b7488674789fd49cd0698a60403347bc2168cd5de0a8491349b7`; roles: exported-object
- sha256: `327eb44a247ac6e38b3d02b76dcdbdaf66a7c7064bf4f3c9fdfd4484a80452ce`; roles: exported-object
- sha256: `32c47cc6b8a9063141d7559f8c0a4c356571b38bba3864d454029bd2c2f0ffde`; roles: exported-object
- sha256: `33421c7d3bc5bae96cfb722a18967bcbbe8ff21e863a802150fe5fbbbdd04ca6`; roles: exported-object
- sha256: `336b14c1f82c04eb8bfd490b73dade0d1a084108f5f43af7d1ab5a5de7e3ccff`; roles: exported-object
- sha256: `3376656a1065f217ece24cf4039aaba336fe35a6c6e29be159fb03cb712ef62d`; roles: exported-object
- sha256: `3443f2dc0c7b74b068d09f28b4ad0e322d341983f4c57893f2eda38427dbd65e`; roles: exported-object
- sha256: `347c0bc98abf0e16e86f72cc7058b8290880c7e089d83d19cbf80aa295e142e6`; roles: exported-object
- sha256: `352dd136c9810049178064b46cf6b149a21cf74198d62455be96509ec710262`; roles: exported-object
- sha256: `35714a390651048138a4be4ddeaceb8234628ae85b8f508f3ef4879adcabac2`; roles: exported-object
- sha256: `384b409d1a3538287c7be92f275d5388cd10d404aac05286d0031e384d110558`; roles: exported-object
- sha256: `38dbf8fe6f99d95e30c7264d7e6bc83d61d675636a461affdc7dedb3bc96439f`; roles: exported-object
- sha256: `3916a0813dfb36961722d081fe5a4835a4e8ccf57258402b6417700b70e71966`; roles: exported-object
- sha256: `3a200099bd79b734329a90776df195da10460140051847e25e839069912dcf1c`; roles: exported-object
- sha256: `3b163eb96641057909fb4f1a4fd2d42771dcf7c8961a4e9d1862e681037afe86`; roles: exported-object
- sha256: `3b967843e46088c05b6f3563768f1046ff9b2a132740ba90c9cb9657632f443a`; roles: exported-object

```

-sha256: `3ba62e70a1c2b45133051bf258188a375751d777542eba48cdb7c6e219d4d052`; roles: exported-object
-sha256: `3c235f28b3544e94b6cb9b106fbed857e46407f2edaeb306ec9f044dc1561c6`; roles: exported-object
-sha256: `3c24ca5e6fc65f64bc89254b7b65a57ce91d2f94a0669264d29cff8b7bee1a6d`; roles: exported-object
-sha256: `3c3fc27182b240f7ef25684b89055f2fb6104216d204c2858ff2f4cc5c5aad73`; roles: exported-object
-sha256: `3c6209fdc3f7b8ab8749023d1c5fd58ac6fcc0cca7f25bedff908e9cb0c32aa5`; roles: exported-object
-sha256: `3cbf196455ce3dc4596ef48d543346ba6019cee0ec3037214ec0e53a023d33db`; roles: exported-object
-sha256: `3cc8277d0766bef38be25da17bc2a547529710bf31e228cdf62b0dac9e218801`; roles: exported-object
-sha256: `3d44c0dfce89c86e116520de3075683d7d7d829e5f450632a37ecccbafda0bdc`; roles: exported-object
-sha256: `3dc4423e315cbeb8e53913228588374f6b5e95c702acd32a1663d0175d92edd0`; roles: exported-object
-sha256: `3edd8e1011fa1e97cdc6dc3d2985ec4ff531fb3ae3c674053341df220b2e4590`; roles: exported-object
-sha256: `3ee2866b868219e05cb89be1f203e90124621837871344428e9c0b2b73a53500`; roles: exported-object
-sha256: `3fa3195a19af437b9c8356765972bb2af3ababab3bb5563fda1770a04b8e0d958`; roles: exported-object
-sha256: `3fb33da40450b7b4c991439b671829118e433f2b30e6a9aa69b9d4e3e21ffd17`; roles: exported-object
-sha256: `3ff8a8023e97907778f39cd4ce45bc69e65f719162ae3a0618a8db425416fd78`; roles: exported-object
-sha256: `40487f3ccbba51bd4740d8e296129781a2d40293cfcff0e8688c6b9c47b48a3e64`; roles: exported-object
-sha256: `415401907436fd5ce187fdaf01b0edd9c25620971a900cd48d396af77ca1cc16`; roles: exported-object
-sha256: `4226968bc416ca4299ceed0b41b92a0bd28ba32dd6964c95919eed35001769ac`; roles: exported-object
-sha256: `42a8a1c74a9fcf27a35963517aae581973e0f89b65bef4cf7bc8bf835364ade1`; roles: exported-object
-sha256: `42b7c8ac10d317ebce9ddcac972286ca8f3cea590d578ae5dc853ceecc946c2a`; roles: exported-object
-sha256: `42bb95c4eb86938a55171e950d23e21b10d70ea15943c2432a6afb54ef163a5`; roles: exported-object
-sha256: `435c771adb307c3456f296da31f2000676759f1481c2484c7ec38751fb153b10`; roles: exported-object
-sha256: `4385a17fa2ce6c83c6079bb0593482b48df5bc4b5bd15f913225d7076d5574f8`; roles: exported-object
-sha256: `43e5e8f4682cf04c0a879423e15449b67785926aaf6bb3752d2c019ebf06e6e3`; roles: exported-object
-sha256: `43fc9856c71f37798d1793f95080fcdcb6925cddc9427b68237453a4f7a6801e`; roles: exported-object
-sha256: `445bca5a135f9179c266dcff83841f82fd4637a22ccc7ae656e4e41e20fc9d16`; roles: exported-object
-sha256: `45100f25534e7567b0d6894478c2fc74a259d0e1938d6ef1c3e152bedbc9275`; roles: exported-object
-exported object `zbBYgukXYxzAF2hZc`; SHA-256 `14b57211308ac8ad2a63c965783d9ba1c2d1930d0cafd884374d143a481f9bf3`; size 59392
0 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 `object26220`; SHA-256 `abca26cf70ef57ef879c81a3b45d9fc5ce4437f54bda65d0170f3f5bae8a54f5`; size 1376 bytes
Static content: `{"content_kind":"script-like-text","features":{"excerpt":"","hex","feature":{"dynamic-evaluation","offset":827}},"inspected_bytes":1376
,"inspection_truncated":false,"interpretation":"Static content only; not proof of execution, intent, or malware family"}`. Not execution proof.
-exported object `Ocklqc.jpg`; SHA-256 `2620bf96201e9f328aee98a74ce5b87f221e761a8b2662974b35f90991404337`; size 719872 bytes
-exported object `%3fOXtd9L=cFNTMFx8k4Sl&WN68=YMSFGVfdS9ONGuAKqerSFa9naGdXyzjeSZBg13KbK94ai8h1oihtuDN4qXdc1YMbgxq
WO7UijFru1VtwMrjOYg==`; SHA-256 `1a281a2d280c6d1f1f205d3f8210057b1b555794f6c12db57e4e8e4816cb9036`; size 5149 bytes
-exported object `object27533`; SHA-256 `4662635889a87f2f39280975ae841f8ff9c51a45cee3c5922e08778dae69b077`; size 1528 bytes
-exported object `object17412`; SHA-256 `004599278fd2775eb468eac406e47dab4e5775c32eeb98a0f7ff21768aa2fddcf`; size 1460 bytes
-exported object `object23470`; SHA-256 `0119adca455bfe449a3b6d30660b9a4fb4d7f9b1a42504166debbe61bc7a1a64`; size 1460 bytes
-exported object `object17433`; SHA-256 `012525bd08b8856409471857cdde9928f6f5505e0eedfdc05880783621712242`; size 1460 bytes
-exported object `object11310`; SHA-256 `02751d70749d493ba1989b74765a1cd1c56294db42c8b7775b3c0172828df4a6`; size 1460 bytes
-exported object `object27642`; SHA-256 `03e81cfa927c6cdce33587023c24bb89f21cf506458598c7624bc61c8d3f8e58`; size 1460 bytes
-exported object `object24152`; SHA-256 `0417dd954d3695d2bf400f237806c505bf8cccf07c44ce9467d98ed4175ea255`; size 1460 bytes
-exported object `object9566`; SHA-256 `04b3ca7f09694f7f1b8e7b71f3503d325b75d3ff938ed24eeb9939714635f0d2`; size 1460 bytes
-exported object `object10926`; SHA-256 `04b4f6035a50b1f58ebddb3f5a3e8cf1949a9b6b36b497c86b2b8c2b91e7ad4f`; size 1460 bytes
-exported object `object24077`; SHA-256 `04ded8bd35a45a9dd08f3cc32056559c2d62739e5edebdaf1be2b5bf6133ea3`; size 1460 bytes
-exported object `object25436`; SHA-256 `051f4c30c5306ffeff3f92010446f0aa0c420978da429cb787c50604c5944174`; size 1460 bytes
-exported object `object21540`; SHA-256 `05497fa07eb6f2ee015c09ace90d0423c20136b9c6e4a52ee3e4c60c376eac3`; size 1460 bytes
-exported object `object17594`; SHA-256 `05b0dc4e3b3623d8fe2e6d653af542f73ce33b8d5461de62b0b113aa5f3caa0`; size 1460 bytes
-exported object `object16434`; SHA-256 `05ba7c0984a69934dba3a41191243d8dc8fd5abf2fea86a4ead813cf2a9d9dee`; size 1460 bytes
-exported object `object11911`; SHA-256 `05dfb38ed78ba413e07d3e01d40dd139683aa9b4715d3f000abc9d95e16205a6`; size 1460 bytes
-exported object `object11550`; SHA-256 `0604cda2873562b6894fce5ef33aab23eeb01abae54bfd1a3ade48e85e54f266`; size 1460 bytes
-exported object `object24129`; SHA-256 `0609a4da54220690f415ac4d27cee84f2eeea7d6a39ae990017ac25889ca2ca54`; size 1460 bytes
-exported object `object21424`; SHA-256 `06af7d2c9ddd3737f67c6789e4fa2610ed99d3d4aeb157e15c9f0b3eab46ceed`; size 1460 bytes
-exported object `object21425`; SHA-256 `08387b61ba8264eeff8f26f5d669b04b28b0ae71ee8ffe4de6852c8c2b9668d3d`; size 1460 bytes
-exported object `object7819`; SHA-256 `08ff66f98bdcf6573485fb6a07e45b72de258edb90706aa75260b1f541a961eb`; size 1460 bytes
-exported object `object9111`; SHA-256 `0965a8861f7f70048f6251a520c65bf2930b3b9265e0e55142aa384f4da36f24`; size 1460 bytes
-exported object `object23590`; SHA-256 `09b156788ec22bd98b36d95565ab19199d442dc653c73ddb3525792130b593`; size 1460 bytes
-exported object `object16612`; SHA-256 `09ba1e573a77d25cfe065aa002a155189ce4f5cbfb0251ab61dc3b5eea9569f5`; size 1460 bytes
-exported object `object23550`; SHA-256 `0a1b9616d1191c67cb63f7b1b8bd9809f43c94a183eb23527df28490ac9666f7`; size 1460 bytes
-exported object `object25308`; SHA-256 `0aa09ec450e32afa62a72eeb252e83ad291b68ed378fb455ee4cb618ba04849a`; size 1460 bytes
-exported object `object11969`; SHA-256 `0b0e4ae56a34d0aa05dca4d67700c3964c649f66bc9d9afd2c430bdb1f063be8`; size 1460 bytes
-exported object `object25385`; SHA-256 `0b500a7b1a98e79df9f948812495251061d45e48ee19eb795810272216b6fbc9`; size 1460 bytes
-exported object `object13663`; SHA-256 `0bd44562868ac54cb8c1043310b8f1d8267e681908bbd1d5e14b27ce796b977d`; size 1460 bytes
-exported object `object23853`; SHA-256 `0ded265abee66125302a95e54828bf136e471f93d1c6ddbaec3513f4960254b6`; size 1460 bytes

```

- exported object `object23927`; SHA-256 `0df6c8212c4a7361f440ffbd61ee76222cbc3d4e24b3c2716946800e13fd8ce8`; size 1460 bytes

- exported object `object17580`; SHA-256 `0e60578c595f5d1d852562e954c270edcaec54de126892ebf8dc2a60c9b1503`; size 1460 bytes

- exported object `object17735`; SHA-256 `0ec2306524e6c599765d5d1223e9a33329d8c0793039e8d26c15de173d79e958`; size 1460 bytes

- exported object `object22136`; SHA-256 `0f102e9552d90e78af23de4a7b4411569878a3149aaebc38e5168e422c5d247e`; size 1460 bytes

- exported object `object10934`; SHA-256 `0f99ac235c51cdf782c4f8193f4698892a38d6365845031d7b20f976196fe4f`; size 1460 bytes

- exported object `object16749`; SHA-256 `0ff8e752caa95643bf7b3776d821737814f87fe3d6925701a3183971391edcf`; size 1460 bytes

- exported object `object23930`; SHA-256 `0ffbddc5bc92b9e3b50893241fa9a182f02ab2a61054568668bec4f2e8a08fe9`; size 1460 bytes

- exported object `object11134`; SHA-256 `10570ef48a963eeab20a1bd339618b44d213b436c19c51fb05099183a9999f4b`; size 1460 bytes

- exported object `object16496`; SHA-256 `10e9248a956dcfbd1d4c8b70dd05ee54605208b614d10ceb7b8b88d150cb0ef`; size 1460 bytes

- exported object `object21251`; SHA-256 `118a94f5308fb6dd5bf0096ef766eb9fdc207a1c05fc23c7186aba49100ee508`; size 1460 bytes

- exported object `object17490`; SHA-256 `120f7dd788fe12ca8c9af5f9d47d1fa963b0f63bc63cef3afcd28ab66bdfb6f`; size 1460 bytes

- exported object `object17178`; SHA-256 `121098e0cde0a928173ac2ba2da6dd82b1b626453b296059c60926787b1e4546`; size 1460 bytes

- exported object `object17210`; SHA-256 `1235888074ede34f4f78e3108c85f05795ab16d8fb72b534547fb0da3e6a234e`; size 1460 bytes

- exported object `object22466`; SHA-256 `129c768192359093317c1b658b106ba3d9968476a695fef49ea9e6d118467767`; size 1460 bytes

- exported object `object26286`; SHA-256 `139f6fa785927256480056be4662ba4122fa4e5a18d7b63752f8d2ae6c9395b6`; size 1460 bytes

- exported object `object11872`; SHA-256 `13bf0aa04849e77d7914f426c28a54bb49f547cc004ae800af68864980a4a88d`; size 1460 bytes

- exported object `object13662`; SHA-256 `14245b645e4103d8713ef7f916fc7d4d10ae98146a05af38d2b800d52c8acc171`; size 1460 bytes

- exported object `object24538`; SHA-256 `142855918acb873018e7afb636a8f9d0495b3028b4d16b4cf706d68b3a7f8ce3`; size 1460 bytes

- exported object `object16912`; SHA-256 `147f4226dc3c57cb9d2536c745013d7145af769c26fc6b37d0848a01af884865`; size 1460 bytes

- exported object `object17734`; SHA-256 `148dd3a46202949f4ff34c20da8804f68644abec319cbfd57efb774b9b3ebf5d`; size 1460 bytes

- exported object `object16512`; SHA-256 `14a5cc536d16a41573e57bfe68ede705cb5850500eaa5ec123c42784903055c0`; size 1460 bytes

- exported object `object11546`; SHA-256 `14c39252741654b6e9872383aa869070317abb18e91f2d5dbbb1341b3abe62c4`; size 1460 bytes

- exported object `object26741`; SHA-256 `14cd9376ff8f1a914c40168783efb3d4e8f53c2526378000a0190478621eac9f`; size 1460 bytes

- exported object `object21920`; SHA-256 `157889eb6bfcd5fb11eca24228c4f9ae1a176455785456ca79849fb0bb5c2792`; size 1460 bytes

- exported object `object16587`; SHA-256 `15861b469b40931e7dbe3a8b6aach1ee6824b431fea25281840e1db28086d255`; size 1460 bytes

- exported object `object16905`; SHA-256 `161004698346c45313eef873dc3e555f83bf5f4fd61d1f67947fbc8cf3b2660`; size 1460 bytes

- exported object `object11466`; SHA-256 `1694f0ee7be6029fe279792606f74d0e0c156eedf216eb6d30753048e33ac95c`; size 1460 bytes

- exported object `object16517`; SHA-256 `16f02f7a9a59c59bf6b7651c334043da2c43d100661c8345dce857c8743374b0`; size 1460 bytes

- exported object `object14759`; SHA-256 `178252c182d98d603e7235df45e57e1d92aa93fc0c3b71d5c27bc1b7b1c7c310`; size 1460 bytes

- exported object `object16254`; SHA-256 `178ca47275e40b28d97e3f2445c90926cecad89d7679ee5eb59cd1917041f61e`; size 1460 bytes

- exported object `object21272`; SHA-256 `18ce8668476bb27422129bf09e3992cafb555779513b7c73daa5e1b07577dbf1`; size 1460 bytes

- exported object `object10754`; SHA-256 `191a086e159061a0c87247adcf0e042e6c15854fca15397fe2dc99a0f35efa1ed`; size 1460 bytes

- exported object `object21917`; SHA-256 `195aaab78e060cb793d406f91c91592c44a15d944ae7662a5fd8dc7750a121dd`; size 1460 bytes

- exported object `object16797`; SHA-256 `1970d832434fda01ee77325d7882f19089ff3dc6b6e623be0e2be3e21da60290`; size 1460 bytes

- exported object `object16273`; SHA-256 `199efb2dba801fbe4f06b60162b3cc083a63d6078f6b56224f5dc538ded3bdf4`; size 1460 bytes

- exported object `object16871`; SHA-256 `1a188e05405f1ce01789dc73de2d60632eade6ad95ff36cec29b988444861eb1`; size 1460 bytes

- exported object `object16257`; SHA-256 `1bc147f6a38ee4f00397689ae7cbaae2a9807b40d9092404c90dbe97611ab079`; size 1460 bytes

- exported object `object16374`; SHA-256 `1c0c79371604a7e57f527a518397cbbfc312314c6213ac27b44d3a62abd87f17`; size 1460 bytes

- exported object `object25354`; SHA-256 `1c19ebc675280676ea53db434f16e8f1b97b729785511d5c82ebb610fb53f08d`; size 1460 bytes

- exported object `object17272`; SHA-256 `1c3694a1647d000fce54a9d5a30c1a06da57a9e6fab75870993b4d5653577417`; size 1460 bytes

- exported object `object27275`; SHA-256 `1cd3bcddfa4cebaeba570316c23a0248dfb1dd90898bca8e1bf01596b5beedcc`; size 1460 bytes

- exported object `object21299`; SHA-256 `1d16bd195b28177d0030375134b90eab863a25458c56d05c7e72ecfcdad8ddf8`; size 1460 bytes

- exported object `object14756`; SHA-256 `1d21900f027764a25c787c4e444214277ab36e2074037e5d5a8ce6f0efbb004e`; size 1460 bytes

- exported object `object11261`; SHA-256 `1d71eef40b1c844cb461ecc7197ed8eef6bc582ba1e5dc287c3bf5fc15e1b4af`; size 1460 bytes

- exported object `object17680`; SHA-256 `1db156538dd79f08b09c654f86b8f6d481d588fa44cc51f02c4e42fcdca7913`; size 1460 bytes

- exported object `object8253`; SHA-256 `1de41672c3a500d7321663f486920a8fb5f29e8801f92be3e1aa60cb78dbdbf7`; size 1460 bytes

- exported object `object10548`; SHA-256 `1f0fd84ce2a8a3ae572963ae3ad0937920664b081fe79ac87fde2b13acc77be`; size 1460 bytes

- exported object `object16737`; SHA-256 `1f68d99e75eaded0dbd08ee26e222e4a21040c56a6266f1d0d9b385730ca12fc0`; size 1460 bytes

- exported object `object25391`; SHA-256 `1fe5730bb3502850c53ca50dc874702126977f857a47c3dbe5d1a1226afd5c08`; size 1460 bytes

- exported object `object16725`; SHA-256 `206abeeaebf598ad3c984ba9e8b3d56d663989b35c5074ef330514b5841e1a6e`; size 1460 bytes

- exported object `object17689`; SHA-256 `209565664129ec0b9c01867286aa093f1ca15e4ad12093aac53bc290925ae39f`; size 1460 bytes

- exported object `object8292`; SHA-256 `211aa041d8b4ea3a643d44eb8f538f6caa0a5e0e3b63a802de33fbf0a9011a1f1`; size 1460 bytes

- exported object `object23923`; SHA-256 `2143e3b14753fe28b4e495e57c087ef8fea10cbd644761105d607d90b9d23633`; size 1460 bytes

- exported object `object17692`; SHA-256 `2194c3bdb83d8e73218ec1fc36977bd7566500eb0cc264750ce08248f7575543`; size 1460 bytes

- exported object `object7549`; SHA-256 `21abcfcccf584af261252953ef89fd36141f086a365fbd9d2066ae94b3c4bd76`; size 1460 bytes

- exported object `object23085`; SHA-256 `2251efee138848fe36171baae0d12828489e0bcc3b063bc509e2724cf671c01f`; size 1460 bytes

- exported object `object11399`; SHA-256 `2269981a9b387528f38aaa58c273b3a203ba1ce1e4ab7d369210e411cedaef46`; size 1460 bytes

- exported object `object24672`; SHA-256 `22704106a20c5a5a5f4c78a113092eade0f683945a2496a9a0d5bc69c52bd814`; size 1460 bytes

- exported object `object16263`; SHA-256 `2321ba015f0e7a3d74e190c407ecc25f0b772956eb0645036818a324965264ee`; size 1460 bytes

- exported object `object25375`; SHA-256 `2330b96b60d76e24f5bfcc6d9a4e415cb57d4a8c18d95d50566701d112ab2ca9`; size 1460 bytes

- exported object `object24844`; SHA-256 `23f00aaf4245b4855825f38da30d464bef3c6f81eea7235c99fc7bd5d6b726a3`; size 1460 bytes

- exported object `object17105`; SHA-256 `23f6e432c83a9a3dcb731391e864afb6129df0a7eedda745e7cc51baf1ea1ad2`; size 1460 bytes

- exported object `object11458`; SHA-256 `248430bf42f12f2b4e703bb156543d496f2890ad08148d590f93348830c1ad52`; size 1460 bytes

- exported object `object21888`; SHA-256 `24ec4098e828c89dfb5810b1e4df67cd3e8987e672b16a393e1045ba3ded185e`; size 1460 bytes

- exported object `object10704`; SHA-256 `24feb82784833ef28e43907591d6823fb703d92e6a3960435bea7934a35f15e1`; size 1460 bytes

- exported object `object11569`; SHA-256 `253dd1918125d171a4877950898de2ca26060c40b1d05c8fe31cc9fb56776472`; size 1460 bytes

- exported object `object11545`; SHA-256 `25911c516fcaaded9ea55ede4e30828fe8e21e9a895f5e8948034e9621343854`; size 1460 bytes

- exported object `object22695`; SHA-256 `263bc7831746b36b6903d8f193117e6f1e777b2e8765086740b8c0b2af19630e`; size 1460 bytes

- exported object `object12127`; SHA-256 `26d630a69965af7110e23e7d89e870aa432f466b8e25d825ba90a1d615b74765`; size 1460 bytes

- exported object `object10927`; SHA-256 `2741234de895bed810734f6b55872a58fc208957ab25ecea14b7aed45f7c5726`; size 1460 bytes

- exported object `object21048`; SHA-256 `274e7318a4440240d24701135a3a037ffc4064ab6e18b7683968d7ad7557823c`; size 1460 bytes

- exported object `object10936`; SHA-256 `2756bae8f350efe025c1a19b8c04b741660f265fa60d9accbdcee7575d65a301`; size 1460 bytes

- exported object `object23410`; SHA-256 `276fdf588903250404f05a86da40c2e5c26360c7dd2cfce409d8eaf30640e1e6`; size 1460 bytes

- exported object `object9386`; SHA-256 `28204d9f1d7b8c17b7cd049bf732b5dc41e538ad9c17d884c1e06eab2d8dd39`; size 1460 bytes

- exported object `object17777`; SHA-256 `28c04e7c2529f941c2276321566ed73a1cd75404e1b419a0ed1afe2ef1e4bb5c`; size 1460 bytes

- exported object `object11451`; SHA-256 `29804a73896b8364000f4c23c69de02f4b4305e30f21c39a39097ac982863ee8`; size 1460 bytes

- exported object `object23095`; SHA-256 `29a06c4b40fada661ba0e4f26673529c42d9bd1fff629bfed06cdea351634ae`; size 1460 bytes

- exported object `object22946`; SHA-256 `29b84a0556ab8203d2e5fde7529491a0253e9586cf9506583cf50acf715f08cc`; size 1460 bytes

- exported object `object26524`; SHA-256 `29bce0e3976c1a4b0c5a3dedaf4c1df15560fed60eefc170b4e8f1bfd72e881e`; size 1460 bytes

- exported object `object17748`; SHA-256 `2a223bc66bee6f01307afacca8cd03c762c109e39095bf5329d7d70920cdf601`; size 1460 bytes

- exported object `object18886`; SHA-256 `2b785b0137066ea6c9bcb8baa757e5633539962796080eeb05ccdd3d775f40845`; size 1460 bytes

- exported object `object11115`; SHA-256 `2b79250e166209b04e6221f70295861958a9388503c781ddd638cc3864843f5a`; size 1460 bytes

- exported object `object17615`; SHA-256 `2b999f47b936dc400728793101b43657b4e9410a7267fb92cd15fac90fd2a482`; size 1460 bytes

- exported object `object7437`; SHA-256 `2ba817fc45b0dec23acca80833f3e7d19a99b3fc71f3e2fa673ef4c38cf533c`; size 1460 bytes

- exported object `object12132`; SHA-256 `2c1b8be8a085bd2d29dc9c0fdc032117a77193dad38602390554138f7cdf4cf`; size 1460 bytes

- exported object `object22156`; SHA-256 `2cc04e0598d2938235c3ef5eeca39c65285f0dcb3149c70fc0a7362a4ea3f490`; size 1460 bytes

- exported object `object17468`; SHA-256 `2d3a83cf33a1a7bbe0b8d0d003e520924b0aa95732828cc17290fb9d461ab96b`; size 1460 bytes

- exported object `object11999`; SHA-256 `2d4829a665a6465d8a67a009389b86e8068c01ce3d094f0459de4ed54ef2199`; size 1460 bytes

- exported object `object16315`; SHA-256 `2d4c01d66de1641649052c860fd1a8788f5193f3db96487f4f2d6d82a35d6d07`; size 1460 bytes

- exported object `object24106`; SHA-256 `2de61824c9fdc4a84764dee59289619829a98149225fc246989abfd4dfcd5913a`; size 1460 bytes

- exported object `object11971`; SHA-256 `2df0449ed47af8473fb17afa4cdfbf3ed4b11a0df006bc7b090fe4f4f74b59f`; size 1460 bytes

- exported object `object16563`; SHA-256 `2e24ef287ea02c7f4c4cc2826389e7b69d3d559d35adbcbbdc9b3d7437bd772f5`; size 1460 bytes

- exported object `object17774`; SHA-256 `2e3c4533bd6dbe6301f70359c32ff7b03f3c6599208e18fec224196b77ae633d`; size 1460 bytes

- exported object `object21024`; SHA-256 `2ef86698bfc9c4ce9dacd4733967d03b4b58e2130c0905f1ae479e689c767234`; size 1460 bytes

- exported object `object22062`; SHA-256 `2f41a6bbfe2c57b767df989d53cad14278bcaa7b0fe886f8c6b1e7f0cab3c019`; size 1460 bytes

- exported object `object11479`; SHA-256 `2f6d5d053ebbfcb3abd90f94bc862175c2782dd5cc60fb9dbb82a2fe9e8ebaf2`; size 1460 bytes

- exported object `object21961`; SHA-256 `311456b3d2193c6a82531c7338dba44beae1363a17ecfcae9ead85549f3f666`; size 1460 bytes

- exported object `object23442`; SHA-256 `311b06d1311f38632a53291a497a27877e1d9bed83ed7d344fb3110938ceb1fa`; size 1460 bytes

- exported object `object122055`; SHA-256 `313ac03b87cec74ab7068a0c183daed376e45377fa754059eb752e64fa5c5186`; size 1460 bytes

- exported object `object22064`; SHA-256 `31b2c11ae258a1e49a65bfc346e74b260221370dcd5ccf9f3761399de9f71b3d`; size 1460 bytes

- exported object `object17181`; SHA-256 `31f63b033376b7488674789fd49cd0698a60403347bc2168cd5de0a8491349b7`; size 1460 bytes

- exported object `object8754`; SHA-256 `327eb44a247ac6e38b3d02b76dcdcbdaf66a7c7064bf4f3c9f9fd4484a80452ce`; size 1460 bytes

- exported object `object26365`; SHA-256 `32c47cc6b8a9063141d7559f8c0a4c356571b38bba3864d454029bd2c2f0ffde`; size 1460 bytes

- exported object `object9380`; SHA-256 `33421c7d3bc5bae96cfb722a18967bcbbe8ff21e863a802150fe5fbbbdd04ca6`; size 1460 bytes

- exported object `object17514`; SHA-256 `336b14c1f82c04eb8bfd490b73dade0d1a084108f5f43af7d1ab5a5de7e3ccff`; size 1460 bytes

- exported object `object16485`; SHA-256 `3376656a1065f217ece24cf4039aaba336fe35a6c6e29be159fb03cb712ef62d`; size 1460 bytes

- exported object `object22208`; SHA-256 `3443f2dc0c7b74b068d09f28b4ad0e322d341983f4c57893f2eda38427dbd65e`; size 1460 bytes

- exported object `object11525`; SHA-256 `347c0bc98abf0e16e86f72cc7058b8290880c7e089d83d19cbf80aa295e142e6`; size 1460 bytes

- exported object `object25421`; SHA-256 `352dd136c9810049178064b46cfeb6149a21cf74198d62455be96509ec710262`; size 1460 bytes

- exported object `object16734`; SHA-256 `35714a390651048138a4be4ddeaceb8234628ae85b8f508f3ef4879adcabacb2`; size 1460 bytes

- exported object `object16216`; SHA-256 `384b409d1a3538287c7be92f275d5388cd10d404aac05286d0031e384d110558`; size 1460 bytes

- exported object `object21421`; SHA-256 `38dbf8fe6f99d95e30c7264d7e6bc83d61d675636a461affdc7dedb3bc96439f`; size 1460 bytes

- exported object `object23852`; SHA-256 `3916a0813dfb36961722d081fe5a4835a4e8ccf57258402b6417700b70e71966`; size 1460 bytes

- exported object `object16789`; SHA-256 `3a200099bd79b734329a90776df195da10460140051847e25e839069912dcf1c`; size 1460 bytes

- exported object `object16322`; SHA-256 `3b163eb96641057909fb4f1a4fd2d42771dcf7c8961a4e9d1862e681037afe86`; size 1460 bytes

- exported object `object22152`; SHA-256 `3b967843e46088c05b6f3563768f1046ff9b2a132740ba90c9cb9657632f443a`; size 1460 bytes

- exported object `object17273`; SHA-256 `3ba62e70a1c2b45133051bf258188a375751d777542eba48cdb7c6e219d4d052`; size 1460 bytes

- exported object `object17421`; SHA-256 `3c235f28b3544e94b6cb9b106fbcd857e46407f2edaab306ec9f044dc1561c6`; size 1460 bytes

- exported object `object22858`; SHA-256 `3c24ca5e6fc65f64bc89254b7b65a57ce91d2f94a0669264d29cfff8b7bee1a6d`; size 1460 bytes

- exported object `object11547`; SHA-256 `3c3fc27182b240f7ef25684b89055f2fb6104216d204c2858ff2f4cc55aad73`; size 1460 bytes

- exported object `object23850`; SHA-256 `3c6209fdc3f7b8ab8749023d1c5fd58ac6fcc0cca7f25bedff908e9cb0c32aa5`; size 1460 bytes

- exported object `object17435`; SHA-256 `3cbf196455ce3dc4596ef48d543346ba6019cee0ec3037214ec0e53a023d33db`; size 1460 bytes

- exported object `object8057`; SHA-256 `3cc8277d0766bef38be25da17bc2a547529710bf31e228cdf62b0dac9e218801`; size 1460 bytes

- exported object `object9465`; SHA-256 `3d44c0dfce89c86e116520de3075683d7d7d829e5f450632a37eccbafda0bdc`; size 1460 bytes

- exported object `object28195`; SHA-256 `3dc4423e315cbeb8e53913228588374f6b5e95c702acd32a1663d0175d92edd0`; size 1460 bytes

- exported object `object25402`; SHA-256 `3edd8e1011fa1e97cdc6dc3d2985ec4ff531fb3ae3c674053341df220b2e4590`; size 1460 bytes

- exported object `object7902`; SHA-256 `3ee2866b868219e05cb89be1f203e90124621837871344428e9c0b2b73a53500`; size 1460 bytes

- exported object `object24486`; SHA-256 `3fa3195a19af437b9c8356765972bb2af3ababa3bb5563fda1770a04b8e0d958`; size 1460 bytes

- exported object `object24104`; SHA-256 `3fb33da40450b7b4c991439b671829118e433f2b30e6a9aa69b9d4e3e21ffd17`; size 1460 bytes

- exported object `object17228`; SHA-256 `3ff8a8023e97907778f39cd4ce45bc69e65f719162ae3a0618a8db425416fd78`; size 1460 bytes

- exported object `object18660`; SHA-256 `40487f3ccba51bd4740d8e296129781a2d40293fcff0e8688c6b9c47b48a3e64`; size 1460 bytes
 - exported object `object16647`; SHA-256 `415401907436fd5ce187fdaf01b06dd9c25620971a900cd48d396af77ca1cc16`; size 1460 bytes
 - exported object `object17114`; SHA-256 `4226968bc416ca4299ceed0b41b92a0bd28ba32dd6964c95919eed35001769ac`; size 1460 bytes
 - exported object `object24858`; SHA-256 `42a8a1c74a9fcf27a35963517aae581973e0f89b65bef4cf7bc8bf835364ade1`; size 1460 bytes
 - exported object `object10748`; SHA-256 `42b7c8ac10d317ebce9ddcac972286ca8f3cea590d578ae5dc853ceec946c2a`; size 1460 bytes
 - exported object `object6726`; SHA-256 `42bb95c4eb86938a55171e950d23e21b10d70ea15943c2432a6afb5f4ef163a5`; size 1460 bytes
 - exported object `object16237`; SHA-256 `435c771adb307c3456f296da31f2000676759f1481c2484c7ec38751fb153b10`; size 1460 bytes
 - exported object `object17792`; SHA-256 `4385a17fa2ce6c83c6079bb0593482b48df5bc4b5bd15f913225d7076d5574f8`; size 1460 bytes
 - exported object `object21854`; SHA-256 `43e5e8f4682cf04c0a879423e15449b67785926aaf6bb3752d2c019ebf06e6e3`; size 1460 bytes
 - exported object `object21420`; SHA-256 `43fc9856c71f37798d1793f95080fdbcdb6925cddc9427b68237453a4f7a6801e`; size 1460 bytes
 - exported object `object17350`; SHA-256 `445bca5a135f9179c266dcff83841f82fd4637a22ccc7ae656e4e41e20fc9d16`; size 1460 bytes
 - exported object `object22139`; SHA-256 `45100f25534e7567b0d6894478c2fcf74a259d0e1938d6ef1c3e152bedbc9275`; size 1460 bytes
 - exported object `object28025`; SHA-256 `4555fab8ca58e6531304dbf84796b86c0a8aeb95708120c29191f52d26c4ae7a`; size 1460 bytes
 - exported object `object23825`; SHA-256 `458cf2b38545678d1498b3421a870e90f30d351db27e24179a6763846ff23d19`; size 1460 bytes
 - exported object `object9345`; SHA-256 `45974b10e99ee53cbd42b5c87ecd4f1b95d7d0e55deec332973245d450df28ee`; size 1460 bytes
 - exported object `object26211`; SHA-256 `45cc01eea937401159bab02926bc7c8fa12b6abd5edbe27e84662ee6e2f4a78`; size 1460 bytes
 - exported object `object23401`; SHA-256 `46e2824454f8e01957f504c3ea01016f6e4e55e313cae11814c23931a7d3694`; size 1460 bytes
 - exported object `object16839`; SHA-256 `46f4a99d212ea9ee939197ff520853f8ce77a42cb3d927ff8e30b083e481c995`; size 1460 bytes
 - exported object `object16250`; SHA-256 `470265729c00e3bcbda9f914676782eb091be09a456a33e3fedc7baf31a4016c`; size 1460 bytes
 - exported object `object18776`; SHA-256 `470566239f44e73efae1810cec3843e5febe44fd291bfbede8addc4f3c446be`; size 1460 bytes
 - exported object `object22920`; SHA-256 `4827626c1838692796d0f167b74b839d36668d4dff4858f71ac7a9cb71816a9d`; size 1460 bytes
 - exported object `object16690`; SHA-256 `483e04ca9f7fb302c5dd99db40bb808a64c04248218362a86d73a96f4354ab1b`; size 1460 bytes
 - exported object `object11785`; SHA-256 `48bd20a01954fbab1004775b2dab614c0263b425e5c2ddaa634a7172a03f1bad`; size 1460 bytes
 - exported object `object23431`; SHA-256 `48c2f29bc316db8422e221b3fd10dc1560eda97df6d5f465f6e1a077f92a527d`; size 1460 bytes
 - exported object `object16731`; SHA-256 `48e600b7724a48ec70eba63611a2d56b390a0c3a6879946b25e604f573abf59f`; size 1460 bytes
 - exported object `object16531`; SHA-256 `493f648828927027e221562702d50127b5666dec98de5c51008f342bdbc3f6102`; size 1460 bytes
 - exported object `object13914`; SHA-256 `496dff3fb8bc99c8d9b06d06831c28e36fa4c23090034654ccb35d3c8ed91581`; size 1460 bytes
 - exported object `object4765`; SHA-256 `49e4663867cb56cd43920fb62bd661c360fdbbba47a4192105c6e5131138b1a0`; size 1460 bytes
 - exported object `object22686`; SHA-256 `4bad85e1a0939636cd9279ff7e57378973d6871337d78d1d8b133694656a3e20`; size 1460 bytes
 - exported object `object16621`; SHA-256 `4bc2d63ee2dd6106fb98a65debb9630a485b2c3d1cec7ae9e79b604307583dc2`; size 1460 bytes
 - exported object `object24139`; SHA-256 `4bdf2e59647db894d51afb06855b310b1ee57c2ddc04a411002681d0dc3d7f10`; size 1460 bytes
 - exported object `object23658`; SHA-256 `4c5231a06021c2fa48a0a9d5e98b3d703a0cfa9dc99257d89146ea79712f6df9`; size 1460 bytes
 - exported object `object7871`; SHA-256 `4cea0c8974225cb7875e6c44d41fb0138d0ce2b92bde96161c3569ff5730c07a`; size 1460 bytes
 - exported object `object16511`; SHA-256 `4cebf9ed49197981b171430848037b9115e2d361f5d33fefe4ae85912ff69772`; size 1460 bytes
 - exported object `object8843`; SHA-256 `4d2d2217e048300dd1f29754b980ed31c578404e59bc93078be9b5c38f22ea08`; size 1460 bytes
 - exported object `object16736`; SHA-256 `4d9180d2c2d43c67c8347589226fa9cae45fb9a94d35c04ad732e7187bd05ff5`; size 1460 bytes
 - exported object `object21843`; SHA-256 `4de5765591e01487bc7f0e2d135b3a3158603eda8c6016aa8576a7ea2ad7dbfd`; size 1460 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: `27cd896e9110b1fda7f2da6c5f4df9153ce2ef635709a10b488145ec018823aa`; recorded 2026-09-19T12:09:25.907745+00:00; mode : local-only.

Coverage: `{"matched\_observables":0,"no\_exact\_match":2994,"observable\_limit":5000,"observables\_checked":2994,"observables\_total":2994,"prior\_case\_limit\_reached":false,"prior\_cases\_checked":11,"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 `6df36b51-4b44-4660-b534-2fa89705e807` shares 31 observations. This does not establish a common campaign.
 - Prior analysis `29aa3ef8-47c9-4c47-b4cc-1ff3e0708142` shares 24 observations. This does not establish a common campaign.
 - Prior analysis `b79032a8-d69e-4ac1-bdd4-542473fa8e3b` shares 36 observations. This does not establish a common campaign.

- Prior analysis `faf041c3-70e0-4a01-8780-10917e5e187c` shares 28 observations. This does not establish a common campaign.
- Prior analysis `08324647-35af-4af2-8d82-4387eec03918` shares 26 observations. This does not establish a common campaign.
- Prior analysis `616a90fa-f15e-4fcb-8d56-7b8e0eff5785` shares 13 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 26 observations. This does not establish a common campaign.
- Prior analysis `38851ad7-b3a0-423d-ae89-3b7be4e4b908` shares 29 observations. This does not establish a common campaign.
- Prior analysis `bfccc426-aa9b-4007-8558-a66d37ecb90c` shares 44 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": 2136, "complete": true, "detailed_objects": 500, "exported_objects": 2638, "hashed_bytes": 4922527, "hashed_objects": 2638, "omitted_unique_hashes": 0, "returned_unique_hashes": 2636, "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": 2636 }`. 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 57/57, identities 14/14, observables 500/2994, artifacts 200/500. Full returned inventory is in the JSON result.