

[SOC-AI-AGENT]

Automated Investigation Report

Alert ID: 9cc13d01-c662-4ff0-bffd-731db58dfc8b | Generated: 2026-02-13 04:17:15 UTC

Executive Summary

Verdict: FALSE_POSITIVE (90.0% confidence) — benign activity (false positive). Key factors: No IOCs flagged as malicious by enrichment sources. IOCs appeared in 1 false positive(s). May reduce malicious confidence.

Verdict

Confidence: 90.0%

Alert Details

Field	Value
Alert Type	generic
Timestamp	2024-01-15T10:30:01.042000+00:00
Classification	c2_communication
Initial Severity	MEDIUM

Investigation Timeline

Triage — Complete

Classified as c2_communication. Severity: MEDIUM.

IoC Extraction — Complete

Extracted 30 IOCs: {'domain': 30}

Enrichment — Complete

Enriched 30 IOCs across threat intel sources.

Correlation — Complete

Found 1 related investigation(s). Shared IOCs: a3jhzgvulm1hbgljzs5jb20uyxvzdhjhbg1h.data.c2-exfil.xyz (seen 1x). 1 related investigation(s) were previously classified as false positives.

Att&ck Mapping — Complete

Matched 0 techniques across 0 tactics.

Verdict — Complete

FALSE_POSITIVE (confidence: 90.0%)

IOC Enrichment Results

IOC	Type	Risk Score	Sources Flagged	Summary
a3jhzgvulm1hbgljzs5jb20uyxvzdhjhbg1h.data.c2-exfil.xyz		0 / 4		VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
dxnlcm5hbwu9amrvzsww29yzd1qqhnz.dat		0 / 4		VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
d29yzde9ywrtaw4mc2vy████████wrjmdeuy29y.dat@.0c2-exfil.xyz		0 / 4		VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
cc5hy2111mxvy2fsjmrv████████j1hy2111mxv.dat@.0c2-exfil.xyz		0 / 4		VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
y2fsjnnpzd1tmi0xltut████████zu0mtqzmdky.dat@.0c2-exfil.xyz		0 / 4		VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
oc0ymduxnzexmjewltez████████dqznjktmtew.dat@.0c2-exfil.xyz		0 / 4		VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
nczudgxtptiwzjhlowex████tm0mjrhmjyy.dat@.0c2-exfil.xyz		0 / 4		VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

				VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
end000.data.c2-exfil	0.0	0 / 4		

Historical Correlation

Found 1 related investigation(s). Shared IOCs: a3jhzgvulm1hbg1jzs5jb20uyxvzdhjhbg1h.data.c2-exfil.xyz (seen 1x). 1 related investigation(s) were previously classified as false positives.

Alert ID	Type	Verdict	Matching IOC	Date
ddb72981...	generic	FALSE_POSITIVE	a3jhzgvulm1hbg1jzs5jb20uyxvzdhjhbg1h.data.c2-exfil.xyz	2026-02-13T03:57:14.912590Z

Reasoning Chain

No IOCs flagged as malicious by enrichment sources.

No significant behavioral indicators detected.

IOCs found in 1 previous investigation(s).

IOCs appeared in 1 false positive(s). May reduce malicious confidence.

No MITRE ATT&CK techniques identified.

No temporal risk factors identified.

Score Breakdown

Component	Score	Weight	Weighted Score

Enrichment	0.0	35.0%	0.0
Behavioral	0.0	25.0%	0.0
Correlation	0	20.0%	0.0
Mitre	0.0	15.0%	0.0
Temporal	0.0	5.0%	0.0

Recommended Response Actions

1. No immediate action required.
2. Consider adding to allowlist/exception list if recurring.
3. Document the false positive for tuning detection rules.

Raw Evidence

```

2024-01-15T10:30:01.042Z query: 10.0.2.105:52341 -> 10.0.0.10:53 TXT
a3JhZGVuLm1hbGljZS5jb20uYXVzdHJhbGlh.data.c2-exfil.xyz NOERROR 0.003s 2024-01-15T10:30:06.118Z
query: 10.0.2.105:52342 -> 10.0.0.10:53 TXT
dXNlcm5hbWU9amRvZSzWYXNzd29yZD1QQHNz.data.c2-exfil.xyz NOERROR 0.002s 2024-01-15T10:30:11.205Z
query: 10.0.2.105:52343 -> 10.0.0.10:53 A
d29yZDE9YWRtaW4mc2VYdmVyPWRjMDEuY29y.data.c2-exfil.xyz NOERROR 0.004s 2024-01-15T10:30:16.331Z
query: 10.0.2.105:52344 -> 10.0.0.10:53 TXT
cC5hY211LmxvY2FsJmRvbWFpbj1hY211Lmxv.data.c2-exfil.xyz NOERROR 0.002s 2024-01-15T10:30:21.402Z
query: 10.0.2.105:52345 -> 10.0.0.10:53 TXT
Y2FsJnNpZD1TMi0xLTUtMjEtMzU0MTQzMdky.data.c2-exfil.xyz NOERROR 0.003s 2024-01-15T10:30:26.519Z
query: 10.0.2.105:52346 -> 10.0.0.10:53 A
OC0yMDUxNzExMjEwLTEzOTEzODQzNjktMTEw.data.c2-exfil.xyz NOERROR 0.002s 2024-01-15T10:30:31.608Z
query: 10.0.2.105:52347 -> 10.0.0.10:53 TXT
NCZudGxtPTIwZjhLOWExYmRjNTM0MjRhMjYy.data.c2-exfil.xyz NOERROR 0.003s 2024-01-15T10:30:36.715Z
query: 10.0.2.105:52348 -> 10.0.0.10:53 TXT
ZWQ3NzI5OGFjYWQ5MzA0YTJiZjA1NzFlZjI2.data.c2-exfil.xyz NOERROR 0.002s 2024-01-15T10:30:41.803Z
query: 10.0.2.105:52349 -> 10.0.0.10:53 A
MGE4MjgxZTliNjQ2NGQ2NjU5NjEyZDMwMzAz.data.c2-exfil.xyz NOERROR 0.004s 2024-01-15T10:30:46.912Z
query: 10.0.2.105:52350 -> 10.0.0.10:53 TXT
MDMwNTMzODMwMzAzMDMwMmQ2NjY5NmM2NTcz.data.c2-exfil.xyz NOERROR 0.002s 2024-01-15T10:30:52.028Z
query: 10.0.2.105:52351 -> 10.0.0.10:53 TXT
NjU3Mjc2NjU3MjJkNjQ2MzMwMzEyZTYxNjM2.data.c2-exfil.xyz NOERROR 0.003s 2024-01-15T10:30:57.109Z

```

```
query: 10.0.2.105:52352 -> 10.0.0.10:53 A
ZDY1MmU2YzZmNjM2MTZjMmQ2MzNhNWM1NzY5.data.c2-exfil.xyz NOERROR 0.002s 2024-01-15T10:31:02.218Z
query: 10.0.2.105:52353 -> 10.0.0.10:53 TXT
NmU2NDZmNzc3MzVjNTM3OTczNzQ2NTZkMzMz.data.c2-exfil.xyz NOERROR 0.004s 2024-01-15T10:31:07.305Z
query: 10.0.2.105:52354 -> 10.0.0.10:53 TXT
MjVjNTI2ZjZmNzQyZjQzNjk2ZDU2MzIyMzMx.data.c2-exfil.xyz NOERROR 0.002s 2024-01-15T10:31:12.420Z
query: 10.0.2.105:52355 -> 10.0.0.10:53 A
NjQ2MTc0NjEzZDMyMzAzMjM0MmQzMMDMxMmQz.data.c2-exfil.xyz NOERROR 0.003s 2024-01-15T10:31:17.512Z
query: 10.0.2.105:52356 -> 10.0.0.10:53 TXT
MTM1NTMzMzUzYTMzMzIzYTMwMzgyNjcNjU3.data.c2-exfil.xyz NOERROR 0.002s 2024-01-15T10:31:22.631Z
query: 10.0.2.105:52357 -> 10.0.0.10:53 TXT
MTcyNjk3NDY5NmY2ZTNkMzEyNjcwNzI2Zjc0.data.c2-exfil.xyz NOERROR 0.004s 2024-01-15T10:31:27.708Z
query: 10.0.2.105:52358 -> 10.0.0.10:53 A
NmY2MzMnMzZDc0NjM3MDI2NjQ2ZjZkNjE2.data.c2-exfil.xyz NOERROR 0.002s 2024-01-15T10:31:32.819Z
query: 10.0.2.105:52359 -> 10.0.0.10:53 TXT
OTZlM2Q2MTYzNmQ2NTJkNjM2ZjcyNzAyZTZj.data.c2-exfil.xyz NOERROR 0.003s 2024-01-15T10:31:37.905Z
query: 10.0.2.105:52360 -> 10.0.0.10:53 TXT
NmY2MzYxNmMyNjY4NmY3Mzc0NmU2MTZkNjUz.data.c2-exfil.xyz NOERROR 0.002s 2024-01-15T10:31:43.018Z
query: 10.0.2.105:52361 -> 10.0.0.10:53 A
ZDQ2NDYzMzAzMTJ1NjE2MzZkNjUyZDYzNmY3.data.c2-exfil.xyz NOERROR 0.004s 2024-01-15T10:31:48.102Z
query: 10.0.2.105:52362 -> 10.0.0.10:53 TXT
MjcwMmU2YzZmNjM2MTZjMjY2OTcwM2QzMTMw.data.c2-exfil.xyz NOERROR 0.002s 2024-01-15T10:31:53.221Z
query: 10.0.2.105:52363 -> 10.0.0.10:53 TXT
MmUzMDJ1MzIyZTMxMzAzNTI2NmQ2MTYzM2Q2.data.c2-exfil.xyz NOERROR 0.003s 2024-01-15T10:31:58.309Z
query: 10.0.2.105:52364 -> 10.0.0.10:53 A
MzAzYTMxMzQzYTMyMzIzYTMzMzMzYTM0MzQz.data.c2-exfil.xyz NOERROR 0.002s 2024-01-15T10:32:03.418Z
query: 10.0.2.105:52365 -> 10.0.0.10:53 TXT
YTM0MzUyNjZmNzMzZDU3Njk2ZTY0NmY3NzHz.data.c2-exfil.xyz NOERROR 0.004s 2024-01-15T10:32:08.505Z
query: 10.0.2.105:52366 -> 10.0.0.10:53 TXT
MjAzMTMwMmUzMDJ1MzEzOTMwMzQzMTJ1MzMz.data.c2-exfil.xyz NOERROR 0.002s 2024-01-15T10:32:13.621Z
query: 10.0.2.105:52367 -> 10.0.0.10:53 A
MTMxMjY2MTZkNjk2YzNkNTc2ZjcyNmI3Mzc0.data.c2-exfil.xyz NOERROR 0.003s 2024-01-15T10:32:18.709Z
query: 10.0.2.105:52368 -> 10.0.0.10:53 TXT
NjE3NDY5NmY2ZTI2NjQ2NTczNmIzZDQ2NDk0.data.c2-exfil.xyz NOERROR 0.002s 2024-01-15T10:32:23.815Z
query: 10.0.2.105:52369 -> 10.0.0.10:53 TXT
ZTQxNGU0MzQ1MmQ1NzUzMzAzNDAwZW5kMDAx.data.c2-exfil.xyz NOERROR 0.004s 2024-01-15T10:32:28.903Z
query: 10.0.2.105:52370 -> 10.0.0.10:53 A end000.data.c2-exfil.xyz NOERROR 0.002s
```