

# [ SOC-AI-AGENT ]

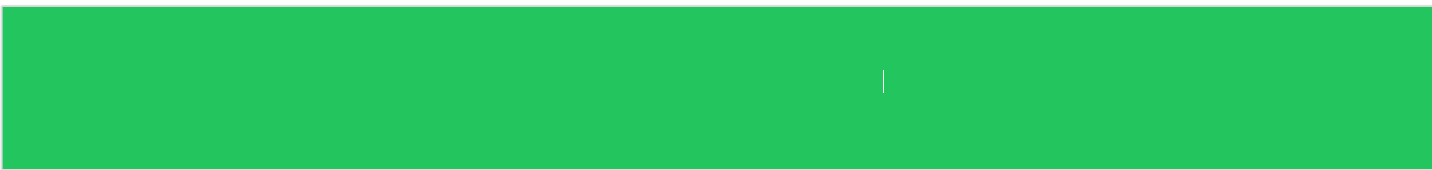
## Automated Investigation Report

Alert ID: ddb72981-3684-4c33-9b40-47501d4a4c19 | Generated: 2026-02-13 04:00:25 UTC

### Executive Summary

Verdict: FALSE\_POSITIVE (90.0% confidence) — benign activity (false positive). Key factors: No IOCs flagged as malicious by enrichment sources.

### 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

No related investigations found. This appears to be a new, isolated alert.

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
a3jhzgvulm1hbg1jzs5j[REDACTED]xvzdhjhbg1h.dat6.0c2-exfil.xyz		6.0	0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
dxnlcm5hbwu9amrvzszw[REDACTED]29yzdlqghnz.dat6.0c2-exfil.xyz		6.0	0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
d29yzde9ywrtaw4mc2vy[REDACTED]wrjmdeuy29y.dat6.0c2-exfil.xyz		6.0	0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

cc5hy21llmxvy2fsjmrvtm0mjrhmjyyjlhy21llmxv.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
y2fsjnnpzdltmi0xltuttm0mjrhmjyyzu0mtqzmdky.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
oc0ymduxnzexmjewltezmqznjktmtew.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
nczudgxtptiwzjhlowexnm0mjrhmjyytm0mjrhmjyy.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

zwq3nzi5ogfjywg5mza0[REDACTED]jalnzflzji2.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
mge4mjgxtlinjq2hgq2[REDACTED]jeyzdmwmzaz.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
mdmwntmzodmwmzazmdmw[REDACTED]jy5nmm2ntcz.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
nju3mjc2nju3mjjknjq2[REDACTED]zeyztyxnm2.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

zdy1mmu2yzzmnjm2mtzj[REDACTED]znhnwm1nzy5.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
nmu2ndzmnzc3mzvjntm3[REDACTED]zq2ntzkmzmz.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
mjvjnti2zjzmnzqyzjqz[REDACTED]du2mziymzmx.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
njq2mtc0njezzdymzaz[REDACTED]mqzmdmxmmqz.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

mtmlntmxmzuzytmzmziz[REDACTED]zgynjcznju3.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
mtcynjk3ndy5nmy2ztnk[REDACTED]jcwnzi2zjc0.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
nmy2mzzmnmzdc0njm3[REDACTED]jq2zjzknje2.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
otzlm2q2mtyznmq2ntjk[REDACTED]jcynzayztzj.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

nmy2mzyxnmmynjy4nmy3[REDACTED]mu2mtzknjuz.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
zdq2ndyzmzazmtjlnje2[REDACTED]juyzdzyzmy3.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
mjcwm2yzzzmnm2mtzj[REDACTED]tcwm2qzmtmw.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
mmuzmdjlmziyztmzmzaz[REDACTED]mq2mtzym2q2.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

mzazytmxmzqzytmymziz[REDACTED]zmzytm0mzqz.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
ytm0mzuynjzmnzmzdu3[REDACTED]ty0nmy3nzhz.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
mjazmtmwmuzmdjlmzez[REDACTED]zqzmtjlmzmz.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
mtmxmjy2mtzknjk2yznk[REDACTED]jcynmi3mzc0.dat0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A



nje3ndy5nmy2zti2njq2[REDACTED]mizzdq2ndk0.data.0.0c2-exfil.xyz			0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
ztqxnngu0mzq1mmq1hzuz[REDACTED]dawzw5kmdax.data.0.0c2-exfil.xyz			0 / 4	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[REDACTED]		0.0	0 / 4	OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

Reasoning Chain

- No IOCs flagged as malicious by enrichment sources.
- No significant behavioral indicators detected.
- No historical correlation data available.
- 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	0.0	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
a3JhZGVuLm1hbG1jZS5jb20uYXVzdHJhbG1h.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
d29yZDE9YWRtaW4mc2VydmVybWVjMDEuY29y.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
cC5hY21lLmxvY2FsJmRvbWVpY21lLmxv.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
Y2FsJnNpZD1TMi0xLTUtMjEtMzU0MTQzMDEy.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
OC0yMDUxNzExMjEwLTExOTQzMDEy.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
MGE4Mjg4ZTliNjQ2NGQ2NjU5NjE5ZDMwMzAz.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
```

