# [ SOC-AI-AGENT ]

Automated Investigation Report

Alert ID: a1dfeff9-6d51-46b7-9d5b-4c63d30b69a4 | Generated: 2026-02-13 04:29:12 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 2 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 2 related investigation(s). Shared IOCs: a3jhzgvulm1hbgljzs5jb20uyxvzdhjhbglh.data.c2-exfil.xyz (seen 2x). 2 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 |
|---|---|---|---|---|
| a3jhzgvulm1hbgljzs5j[redacted]xvzdhjhbglh.data.c2-exfil.xyz | [redacted] | 0.0 | 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 |
| dxnlcm5hbwu9amrvzszw[redacted]29yzd1qqhnz.data.c2-exfil.xyz | [redacted] | 0.0 | 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 |

| | | | | |
|---|---|---|---|---|
| d29yzde9ywrtaw4mc2vy[redacted]wrjmdeuy29y.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |
| cc5hy21llmxvy2fsjmrv[redacted]j1hy21llmxv.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |
| y2fsjnnpzd1tmi0xltut[redacted]zu0mtqzmdky.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |

| | | | | |
|---|---|---|---|---|
| oc0ymduxnzexmjewltez[redacted]dqznjktmtew.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |
| nczudgxtptiwzjhlowex[redacted]tm0mjrhmjyy.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |
| zwq3nzi5ogfjywq5mza0[redacted]ja1nzflzji2.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |

| | | | | |
|---|---|---|---|---|
| mge4mjgxztlinjq2ngq2[redacted]jeyzdmwmzaz.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |
| mdmwntmzodmwmzazmdmw[redacted]jy5nmm2ntcz.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |
| nju3mjc2nju3mjjknjq2[redacted]zeyztyxnjm2.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |

| | | | | |
|---|---|---|---|---|
| zdy1mmu2yzzmnjm2mtzj[redacted]znhnwm1nzy5.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |
| nmu2ndzmnzc3mzvjntm3[redacted]zq2ntzkmzmz.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |
| mjvjnti2zjzmnzqyzjqz[redacted]du2mziymzmx.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |

| | | | | |
|---|---|---|---|---|
| njq2mtc0njezzdmymzaz[redacted]mqzmdmxmmqz.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |
| mtm1ntmxmzuzytmzmziz[redacted]zgynjcznju3.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |
| mtcynjk3ndy5nmy2ztnk[redacted]jcwnzi2zjc0.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |

| | | | | |
|---|---|---|---|---|
| nmy2mzzmnmmzzdc0njm3[redacted]jq2zjzknje2.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 |
| otzlm2q2mtyznmq2ntjk[redacted]jcynzayztzj.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 |
| nmy2mzyxnmmynjy4nmy3[redacted]mu2mtzknjuz.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 |

| | | | | |
|---|---|---|---|---|
| zdq2ndyzmzazmtjlnje2[redacted]juyzdyznmy3.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |
| mjcwmmu2yzzmnjm2mtzj[redacted]tcwm2qzmtmw.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |
| mmuzmdjlmziyztmxmzaz[redacted]mq2mtyzm2q2.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |

| | | | | |
|---|---|---|---|---|
| mzazytmxmzqzytmymziz[redacted]zmzytm0mzqz.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |
| ytm0mzuynjzmnzmzzdu3[redacted]ty0nmy3nzhz.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |
| mjazmtmwmmuzmdjlmzez[redacted]zqzmtjlmzmz.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |

| | | | | |
|---|---|---|---|---|
| mtmxmjy2mtzknjk2yznk[redacted]jcynmi3mzc0.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |
| nje3ndy5nmy2zti2njq2[redacted]mizzdq2ndk0.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |
| ztqxngu0mzq1mmq1nzuz[redacted]dawzw5kmdax.data.c2-exfil.xyz | | | 0 / 4 | VT: 0/93 engines flagged as malicious.<br>Registrar: N/A<br>OTX: 0 pulses reference this IOC. Tags: none<br>WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A |

| | | | | |
|---|---|---|---|---|
| end000.data.c2-exfil[redacted] | | 0.0 | 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 |

## Historical Correlation

Found 2 related investigation(s). Shared IOCs: a3jhzgvulm1hbgljzs5jb20uyxvzdhjhbglh.data.c2-exfil.xyz (seen 2x). 2 related investigation(s) were previously classified as false positives.

| Alert ID | Type | Verdict | Matching IOC | Date |
|---|---|---|---|---|
| ddb72981... | generic | FALSE_POSITIVE | a3jhzgvulm1hbgljzs5j[redacted] | 2026-02-13T03:57:[redacted] |
| 9cc13d01... | generic | FALSE_POSITIVE | a3jhzgvulm1hbgljzs5j[redacted] | 2026-02-13T04:[redacted] |

## Reasoning Chain

No IOCs flagged as malicious by enrichment sources.

No significant behavioral indicators detected.

IOCs found in 2 previous investigation(s).

IOCs appeared in 2 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
cC5hY21lLmxvY2FsJmRvbWFpbj1hY21lLmxv.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
NjQ2MTc0NjEzZDMyMzAzMjM0MmQzMDMxMmQz.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
MTM1NTMxMzUzYTMzMzIzYTMwMzgyNjczNjU3.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
NmY2MzZmNmMzZDc0NjM3MDI2NjQ2ZjZkNjE2.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
ZDQ2NDYzMzAzMTJlNjE2MzZkNjUyZDYzNmY3.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
MmUzMDJlMzIyZTMxMzAzNTI2NmQ2MTYzM2Q2.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
MjAzMTMwMmUzMDJlMzEzOTMwMzQzMTJlMzMz.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
```

---