

[SOC-AI-AGENT]

Automated Investigation Report

Alert ID: 6c4e5364-36e0-4fc6-97cb-7f3e1410c8a7 | Generated: 2026-02-13 04:01:58 UTC

Executive Summary

Verdict: FALSE_POSITIVE (87.30000000000001% confidence) — benign activity (false positive). Key factors: No IOCs flagged as malicious by enrichment sources.

Verdict



Confidence: 87.3%

Alert Details

Field	Value
Alert Type	generic
Timestamp	2024-01-15T22:00:02.418000+00:00
Classification	generic_alert
Initial Severity	MEDIUM
Source IP	91.234.56.78
Destination IP	120.0.0.0

Investigation Timeline

Triage — Complete

Classified as generic_alert. Severity: MEDIUM.

IOC Extraction — Complete

Extracted 3 IOCs: {'url': 1, 'ipv4': 2}

Enrichment — Complete

Enriched 3 IOCs across threat intel sources.

Correlation — Complete

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

Att&ck Mapping — Complete

Matched 1 techniques across 1 tactics.

Verdict — Complete

FALSE_POSITIVE (confidence: 87.3%)

IOC Enrichment Results

IOC	Type	Risk Score	Sources Flagged	Summary
https://91.234.56.78	api/v1/update/check	0.0	0 / 3	
91.234.56.78		10.0	0 / 5	VT: 0/93 engines flagged as malicious. AS: Sc Technological Srl, Country: DE AbuseIPDB: Abuse confidence 0%, 0 reports. ISP: SC TECHNOLOGICAL SRL, Usage: Fixed Line ISP, Country: DE OTX: 0 pulses reference this IOC. Tags: none GreyNoise: IP not observed scanning the internet

120.0.0.0		13.0	0 / 5	VT: 1/93 engines flagged as malicious. AS: CHINA UNICOM China169 Backbone, Country: CN AbuseIPDB: Abuse confidence 8%, 5 reports. ISP: China Unicom Hebei Province Network, Usage: Fixed Line ISP, Country: CN OTX: 2 pulses reference this IOC. Tags: malware GreyNoise: IP not observed scanning the internet
-----------	--	------	-------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

MITRE ATT&CK Mapping

Tactic	Technique ID	Technique Name	Evidence
Execution	T1204.002	User Execution: Malicious File	Enrichment tag: malware

Attack chain analysis:

1. **Execution**: User Execution: Malicious File (T1204.002)

Reasoning Chain

No IOCs flagged as malicious by enrichment sources.

No significant behavioral indicators detected.

No historical correlation data available.

Matched 1 MITRE ATT&CK technique(s) across 1 tactic(s).

Alert occurred during off-hours (22:00). Slightly elevated risk.

Score Breakdown

Component	Score	Weight	Weighted Score
Enrichment	13.0	35.0%	4.5
Behavioral	0.0	25.0%	0.0
Correlation	0.0	20.0%	0.0
Mitre	8	15.0%	1.2
Temporal	20.0	5.0%	1.0

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

```
#Fields: timestamp src_ip src_port dst_ip dst_port method url status_code bytes_sent bytes_recv
user_agent duration #Software: BlueCoat ProxySG Access Log #Version: 1.0 #Date: 2024-01-15
2024-01-15T22:00:02.418Z 10.0.2.47 51203 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 342 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.241
2024-01-15T22:01:04.102Z 10.0.2.47 51204 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 338 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.198
2024-01-15T22:02:01.891Z 10.0.2.47 51205 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 345 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.215
2024-01-15T22:03:05.512Z 10.0.2.47 51206 91.234.56.78 443 POST
```

https://91.234.56.78/api/v1/update/check 200 340 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.232
2024-01-15T22:04:03.208Z 10.0.2.47 51207 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 336 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.187
2024-01-15T22:05:02.617Z 10.0.2.47 51208 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 512 2048 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.452
2024-01-15T22:06:04.891Z 10.0.2.47 51209 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 344 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.204
2024-01-15T22:07:01.305Z 10.0.2.47 51210 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 339 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.221
2024-01-15T22:08:03.718Z 10.0.2.47 51211 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 341 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.195
2024-01-15T22:09:02.104Z 10.0.2.47 51212 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 337 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.238
2024-01-15T22:10:04.520Z 10.0.2.47 51213 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 2048 4096 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.891
2024-01-15T22:15:01.203Z 10.0.2.47 51214 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 340 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.209
2024-01-15T22:16:03.412Z 10.0.2.47 51215 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 343 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.227
2024-01-15T22:17:01.891Z 10.0.2.47 51216 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 338 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.193
2024-01-15T22:18:04.302Z 10.0.2.47 51217 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 341 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.218
2024-01-15T22:19:02.714Z 10.0.2.47 51218 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 336 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.201
2024-01-15T22:20:03.108Z 10.0.2.47 51219 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 8192 16384 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 1.342
2024-01-15T22:30:02.501Z 10.0.2.47 51220 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 344 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.214
2024-01-15T22:31:01.892Z 10.0.2.47 51221 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 339 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.188
2024-01-15T22:32:04.210Z 10.0.2.47 51222 91.234.56.78 443 POST
https://91.234.56.78/api/v1/update/check 200 342 128 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" 0.226
2024-01-15T22:33:02.608Z 10.0.2.47 51223 91.234.56.78 443 POST https://91.234.56.78/api

