Digital Forensic Incident Report

Case ID: 42de4a41

Generated: 2026-01-24 12:49:35 UTC

1. Executive Summary

On 2026-01-24, a single forensic batch was observed in UTC, spanning from 12:48:42.327038 to 12:48:42.330271, a duration of approximately 3.2 milliseconds. The batch contains 16 events originating from five unique source IPs: 79.124.40.174, 198.244.240.150, 92.205.212.128, 216.244.66.199, and 208.167.225.162. The observed event types were PROTOCOL_ABUSE (3 events), WAF_CORRELATION (4 events), SQL_INJECTION (1 event), and ACCESS_DENIED (8 events). Event distribution by source IP: - 79.124.40.174: PROTOCOL_ABUSE × 2 - 198.244.240.150: WAF_CORRELATION × 2; SQL_INJECTION × 1 - 92.205.212.128: ACCESS_DENIED × 3 - 216.244.66.199: WAF_CORRELATION × 2; PROTOCOL_ABUSE × 1 - 208.167.225.162: ACCESS_DENIED × 5 Observations indicate that the batch comprises detections and access-denial events, with no explicit evidence of successful access within the provided data. No attribution or compromise is stated.

2. Chronological Event Timeline

Timestamp (UTC)	Observed Event
2026-01-24 12:48:42.327038+00:00	PROTOCOL_ABUSE detected from 79.124.40.174
2026-01-24 12:48:42.328038+00:00	WAF_CORRELATION detected from 198.244.240.150
2026-01-24 12:48:42.328038+00:00	WAF_CORRELATION detected from 198.244.240.150
2026-01-24 12:48:42.328038+00:00	SQL_INJECTION detected from 198.244.240.150
2026-01-24 12:48:42.328038+00:00	PROTOCOL_ABUSE detected from 79.124.40.174
2026-01-24 12:48:42.329037+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-24 12:48:42.329037+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-24 12:48:42.329037+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-24 12:48:42.329037+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-24 12:48:42.330036+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-24 12:48:42.330220+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-24 12:48:42.330271+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-24 12:48:42.330271+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-24 12:48:42.330271+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-24 12:48:42.330271+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-24 12:48:42.330271+00:00	ACCESS_DENIED detected from 208.167.225.162

3. MITRE ATT&CK; Technique Mapping

Artifact ID	Technique ID	Technique Description
42de4a41	T1048	Exfiltration Over Alternative Protocol
5f35b162	T1046	Network Service Discovery
d013b53c	T1046	Network Service Discovery
6ad03fb9	T1190	Exploit Public-Facing Application
70ed7ff1	T1048	Exfiltration Over Alternative Protocol
6b62e8c9	T1110	Brute Force / Credential Access
43d7e862	T1046	Network Service Discovery
d2cd67c4	T1046	Network Service Discovery
ae6382da	T1048	Exfiltration Over Alternative Protocol
6e6efc47	T1110	Brute Force / Credential Access
7cb170c3	T1110	Brute Force / Credential Access
f9cfd9b8	T1110	Brute Force / Credential Access
43620c3c	T1110	Brute Force / Credential Access
8956955c	T1110	Brute Force / Credential Access
9de8f449	T1110	Brute Force / Credential Access
a2ce6082	T1110	Brute Force / Credential Access

4. Source IP Concentration Analysis

Source IP	Event Count
208.167.225.162	5
198.244.240.150	3
92.205.212.128	3
216.244.66.199	3
79.124.40.174	2

5. Case Intelligence Summary

Attack Channel	Observed
Web	Yes
Authentication	No
Network	No
Endpoint	No
Cloud	No