Digital Forensic Incident Report

Case ID: ad4df229

Generated: 2026-01-24 12:19:01 UTC

1. Executive Summary

A single batch of events was observed within a narrow UTC window from 12:18:05.349425 to 12:18:05.356694. The observed event types were PROTOCOL_ABUSE, WAF_CORRELATION, SQL_INJECTION, and ACCESS_DENIED. Occurrences were distributed across five source IPs, with multiple events coming from individual IPs in rapid succession. No event record explicitly indicated a compromise, and no attribution was recorded in these entries. Per-IP narrative - 79.124.40.174 - PROTOCOL_ABUSE: 2 events at 12:18:05.349425 and 12:18:05.352423 - 198.244.240.150 - WAF_CORRELATION: 2 events at 12:18:05.350424 and 12:18:05.351423 - SQL_INJECTION: 1 event at 12:18:05.351423 - 92.205.212.128 - ACCESS_DENIED: 3 events at 12:18:05.352423, 12:18:05.354693, and 12:18:05.354693 - 216.244.66.199 - WAF_CORRELATION: 2 events at 12:18:05.353422 and 12:18:05.353422 - PROTOCOL_ABUSE: 1 event at 12:18:05.354693 - 208.167.225.162 - ACCESS_DENIED: 4 events at 12:18:05.354693, 12:18:05.355695, 12:18:05.355695, and 12:18:05.356694 Consolidated event counts (batch 1) - PROTOCOL_ABUSE: 3 total events - WAF_CORRELATION: 4 total events - SQL_INJECTION: 1 total event - ACCESS_DENIED: 7 total events Observations - All events occurred within a single second-plus window, with several repeated detections from the same IPs at the same timestamps. - There is no record in this batch that states a system compromise. - No attribution is present for these events in the provided records. If a per-IP summary or a simple counts table would aid further review, I can provide those upon request.

2. Chronological Event Timeline

Timestamp (UTC)	Observed Event
2026-01-24 12:18:05.349425+00:00	PROTOCOL_ABUSE detected from 79.124.40.174
2026-01-24 12:18:05.350424+00:00	WAF_CORRELATION detected from 198.244.240.150
2026-01-24 12:18:05.351423+00:00	WAF_CORRELATION detected from 198.244.240.150
2026-01-24 12:18:05.351423+00:00	SQL_INJECTION detected from 198.244.240.150
2026-01-24 12:18:05.352423+00:00	PROTOCOL_ABUSE detected from 79.124.40.174
2026-01-24 12:18:05.352423+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-24 12:18:05.353422+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-24 12:18:05.353422+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-24 12:18:05.354693+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-24 12:18:05.354693+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-24 12:18:05.354693+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-24 12:18:05.354693+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-24 12:18:05.355695+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-24 12:18:05.355695+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-24 12:18:05.355695+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-24 12:18:05.356694+00:00	ACCESS_DENIED detected from 208.167.225.162

3. MITRE ATT&CK; Technique Mapping

Artifact ID	Technique ID	Technique Description
ad4df229	T1048	Exfiltration Over Alternative Protocol
d5399c63	T1046	Network Service Discovery
c0953a29	T1046	Network Service Discovery
314dc324	T1190	Exploit Public-Facing Application
eac12be9	T1048	Exfiltration Over Alternative Protocol
591ed243	T1110	Brute Force / Credential Access
b6596049	T1046	Network Service Discovery
069f54fb	T1046	Network Service Discovery
debc1c56	T1048	Exfiltration Over Alternative Protocol
9074097b	T1110	Brute Force / Credential Access
6b2016d8	T1110	Brute Force / Credential Access
f13aa8c1	T1110	Brute Force / Credential Access
b263cc62	T1110	Brute Force / Credential Access
47c9869d	T1110	Brute Force / Credential Access
71a65ce3	T1110	Brute Force / Credential Access
a764d63e	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