Digital Forensic Incident Report

Case ID: a76ed473

Generated: 2026-01-24 13:07:12 UTC

1. Executive Summary

During 13:06:10.721818 to 13:06:10.729064 UTC on 2026-01-24, batch 1 events occurred within a narrow 7.2 millisecond window. The events comprise multiple detections from several external IPs, with a mix of protocol-related detections, Web Application Firewall (WAF) correlations, and access-denied results. One instance of SQL injection was flagged within the window. No explicit indication of successful access or system compromise is present in the provided data. Several events are duplicated in time or across the same IP, indicating repeated checks or attempts within milliseconds. Observed event types by source IP: - 79.124.40.174 - PROTOCOL_ABUSE: 2 events - 13:06:10.721818 - 13:06:10.724822 - 198.244.240.150 - WAF_CORRELATION: 2 events - 13:06:10.722818 - 13:06:10.723817 - SQL_INJECTION: 1 event - 13:06:10.723817 - 92.205.212.128 - ACCESS_DENIED: 3 events - 13:06:10.724822 - 13:06:10.726821 - 13:06:10.726821 - 216.244.66.199 - WAF_CORRELATION: 2 events - 13:06:10.725821 - 13:06:10.725821 - PROTOCOL_ABUSE: 1 event - 13:06:10.726821 - 208.167.225.162 - ACCESS_DENIED: 5 events - 13:06:10.727820 (x3) - 13:06:10.728819 - 13:06:10.729064 Aggregate counts by event type: - ACCESS_DENIED: 8 - WAF_CORRELATION: 4 - PROTOCOL_ABUSE: 3 - SQL_INJECTION: 1 Additional notes: - The data show no explicit indication of successful access or system compromise within this window. - Multiple detections and blocks originate from several external IPs in a very tight time frame, including at least one SQL injection flag. - Repetition of events in time or across the same IP suggests repeated checks or attempts within milliseconds. Limitations and conclusions: - No attribution or compromise conclusions are drawn from the provided data. The observations document the detections and timestamps but do not establish a breach or successful intrusion.

2. Chronological Event Timeline

Timestamp (UTC)	Observed Event
2026-01-24 13:06:10.721818+00:00	PROTOCOL_ABUSE detected from 79.124.40.174
2026-01-24 13:06:10.722818+00:00	WAF_CORRELATION detected from 198.244.240.150
2026-01-24 13:06:10.723817+00:00	WAF_CORRELATION detected from 198.244.240.150
2026-01-24 13:06:10.723817+00:00	SQL_INJECTION detected from 198.244.240.150
2026-01-24 13:06:10.724822+00:00	PROTOCOL_ABUSE detected from 79.124.40.174
2026-01-24 13:06:10.724822+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-24 13:06:10.725821+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-24 13:06:10.725821+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-24 13:06:10.726821+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-24 13:06:10.726821+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-24 13:06:10.726821+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-24 13:06:10.727820+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-24 13:06:10.727820+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-24 13:06:10.727820+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-24 13:06:10.728819+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-24 13:06:10.729064+00:00	ACCESS_DENIED detected from 208.167.225.162

3. MITRE ATT&CK; Technique Mapping

Artifact ID	Technique ID	Technique Description
a76ed473	T1048	Exfiltration Over Alternative Protocol
5b27f5df	T1046	Network Service Discovery
fecde5ce	T1046	Network Service Discovery
f38db57e	T1190	Exploit Public-Facing Application
cf19f09e	T1048	Exfiltration Over Alternative Protocol
4c7e71be	T1110	Brute Force / Credential Access
3a081274	T1046	Network Service Discovery
a8b98b75	T1046	Network Service Discovery
3746a1e7	T1048	Exfiltration Over Alternative Protocol
866ff37b	T1110	Brute Force / Credential Access
9e1efac4	T1110	Brute Force / Credential Access
8b81da32	T1110	Brute Force / Credential Access
23dbca31	T1110	Brute Force / Credential Access
ee6b7e7f	T1110	Brute Force / Credential Access
bb58c7b8	T1110	Brute Force / Credential Access
6f98b48d	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