Digital Forensic Incident Report

Case ID: 08abbb43

Generated: 2026-01-25 07:47:21 UTC

1. Executive Summary

Batch 1 observations from 2026-01-25 around 07:46:28 UTC show detections and denials across four IPs, with multiple events occurring within the same second. No successful access events are shown in this batch. The entries span four categories (PROTOCOL_ABUSE, WAF_CORRELATION, SQL_INJECTION, and ACCESS_DENIED). There is no attribution or compromise stated; detections indicate potential probing/attempts and access blocks. Chronological summary of events (timestamp granularity as reported): - 07:46:28.397438 — PROTOCOL_ABUSE — 79.124.40.174 - 07:46:28.398440 — WAF_CORRELATION — 198.244.240.150 - 07:46:28.399439 — PROTOCOL_ABUSE — 79.124.40.174 - 07:46:28.399439 — WAF_CORRELATION — 198.244.240.150 - 07:46:28.399439 — SQL_INJECTION — 198.244.240.150 - 07:46:28.400438 — WAF_CORRELATION — 216.244.66.199 - 07:46:28.400438 — ACCESS_DENIED — 92.205.212.128 - 07:46:28.401437 — PROTOCOL_ABUSE — 216.244.66.199 - 07:46:28.401437 — WAF_CORRELATION — 216.244.66.199 - 07:46:28.402436 — ACCESS_DENIED — 92.205.212.128 - 07:46:28.403436 — ACCESS_DENIED — 208.167.225.162 - 07:46:28.403436 — ACCESS_DENIED — 208.167.225.162 - 07:46:28.404435 — ACCESS_DENIED — 208.167.225.162 Notes: - Some IPs generated multiple events within a single second (e.g., 79.124.40.174 and 208.167.225.162). - The record set does not indicate attribution or compromise; detections align with probing/attempt indicators and subsequent access blocks.

2. Chronological Event Timeline

Timestamp (UTC)	Observed Event
2026-01-25 07:46:28.397438+00:00	PROTOCOL_ABUSE detected from 79.124.40.174
2026-01-25 07:46:28.398440+00:00	WAF_CORRELATION detected from 198.244.240.150
2026-01-25 07:46:28.399439+00:00	WAF_CORRELATION detected from 198.244.240.150
2026-01-25 07:46:28.399439+00:00	SQL_INJECTION detected from 198.244.240.150
2026-01-25 07:46:28.399439+00:00	PROTOCOL_ABUSE detected from 79.124.40.174
2026-01-25 07:46:28.400438+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-25 07:46:28.400438+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-25 07:46:28.401437+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-25 07:46:28.401437+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-25 07:46:28.402436+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-25 07:46:28.402436+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-25 07:46:28.402436+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-25 07:46:28.403436+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-25 07:46:28.403436+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-25 07:46:28.403436+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-25 07:46:28.404435+00:00	ACCESS_DENIED detected from 208.167.225.162

3. MITRE ATT&CK; Technique Mapping

Artifact ID	Technique ID	Technique Description
08abbb43	T1048	Exfiltration Over Alternative Protocol
0e56ee8e	T1046	Network Service Discovery
0a9ca911	T1046	Network Service Discovery
27cb77a4	T1190	Exploit Public-Facing Application
f2b07d43	T1048	Exfiltration Over Alternative Protocol
00fe96fb	T1110	Brute Force / Credential Access
65c018fe	T1046	Network Service Discovery
839ae782	T1046	Network Service Discovery
8b2c382c	T1048	Exfiltration Over Alternative Protocol
87816e87	T1110	Brute Force / Credential Access
2171077b	T1110	Brute Force / Credential Access
6a95f6f7	T1110	Brute Force / Credential Access
43dc0aa9	T1110	Brute Force / Credential Access
1530e603	T1110	Brute Force / Credential Access
8d0004e1	T1110	Brute Force / Credential Access
0ce7fc39	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