Digital Forensic Incident Report

Case ID: 83b17977

Generated: 2026-01-25 08:04:42 UTC

1. Executive Summary

During a very brief interval from 08:03:28.996018 UTC to 08:03:29.003013 UTC, a set of security events was observed. The event tally comprises PROTOCOL_ABUSE (3 events), WAF_CORRELATION (4 events), SQL_INJECTION (1 event), and ACCESS_DENIED (7 events). Source IPs and event associations are as follows: - 79.124.40.174: two PROTOCOL_ABUSE events. - 198.244.240.150: two WAF_CORRELATION events and one SQL_INJECTION event. - 216.244.66.199: two WAF_CORRELATION events and one PROTOCOL_ABUSE event. - 92.205.212.128: two ACCESS_DENIED events. - 208.167.225.162: five ACCESS_DENIED events. Assessment notes indicate that all observed ACCESS_DENIED events are denied attempts, with no explicit successful access reported in these events. There is one SQL_INJECTION detection originating from 198.244.240.150. No attribution or compromise is stated or inferred from the data provided. Overall, the observations show multiple sources generating detections and denial events within a few seconds, including protocol abuse indicators, WAF correlation alerts, and a single SQL injection detection. No evidence of a confirmed compromise is present in the provided data.

2. Chronological Event Timeline

Timestamp (UTC)	Observed Event
2026-01-25 08:03:28.996018+00:00	PROTOCOL_ABUSE detected from 79.124.40.174
2026-01-25 08:03:28.997016+00:00	WAF_CORRELATION detected from 198.244.240.150
2026-01-25 08:03:28.997016+00:00	WAF_CORRELATION detected from 198.244.240.150
2026-01-25 08:03:28.997016+00:00	SQL_INJECTION detected from 198.244.240.150
2026-01-25 08:03:28.998017+00:00	PROTOCOL_ABUSE detected from 79.124.40.174
2026-01-25 08:03:28.998017+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-25 08:03:28.998017+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-25 08:03:28.998017+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-25 08:03:28.999016+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-25 08:03:28.999016+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-25 08:03:28.999016+00:00	ACCESS_DENIED detected from 92.205.212.128
2026-01-25 08:03:29.002014+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-25 08:03:29.002014+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-25 08:03:29.002014+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-25 08:03:29.002014+00:00	ACCESS_DENIED detected from 208.167.225.162
2026-01-25 08:03:29.003013+00:00	ACCESS_DENIED detected from 208.167.225.162

3. MITRE ATT&CK; Technique Mapping

Artifact ID	Technique ID	Technique Description
83b17977	T1048	Exfiltration Over Alternative Protocol
3cede073	T1046	Network Service Discovery
d2bcc3a2	T1046	Network Service Discovery
be11e3fe	T1190	Exploit Public-Facing Application
a5083e6a	T1048	Exfiltration Over Alternative Protocol
815860f1	T1110	Brute Force / Credential Access
6939d9bf	T1046	Network Service Discovery
7c9d8a6b	T1046	Network Service Discovery
a909c8c3	T1048	Exfiltration Over Alternative Protocol
280c6580	T1110	Brute Force / Credential Access
1a81be82	T1110	Brute Force / Credential Access
901ab84d	T1110	Brute Force / Credential Access
d7980687	T1110	Brute Force / Credential Access
f68f1ec9	T1110	Brute Force / Credential Access
8d285c80	T1110	Brute Force / Credential Access
972c350e	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