Digital Forensic Incident Report

Case ID: f6c6c09f

Generated: 2026-01-31 08:20:25 UTC

1. Executive Summary

Across a very short time window on 2026-01-31, a concentrated sequence of detections and access-denied events appeared in the logs. The activity spans four overlapping batches within roughly 20 milliseconds, involving multiple IPs and several detection categories (ACCESS_DENIED, WAF_CORRELATION, PROTOCOL_ABUSE, LFI, and in one case RCE). No explicit compromise is indicated in the provided data, and no attribution is inferred. Batch 1 (approximately 08:18:37.504251–08:18:37.509277 UTC) - Access-denied events from external sources were observed for multiple IPs: - 178.16.55.142 (two events) - 109.234.161.199 - 77.55.253.213 - 103.191.208.118 - 198.54.126.38 - 212.154.119.3 (two events) - 185.73.130.137 - 162.55.240.80 - 143.95.111.157 - 178.128.239.177 - 103.2.225.70 - WAF-related detections (external sources): - 198.244.240.20 - WAF_CORRELATION (two events) - SQL_INJECTION (one event) - 45.195.7.235 - WAF_CORRELATION (two events) - PROTOCOL_ABUSE (one event) - Protocol abuse detected from: - 204.76.203.212 - 45.195.7.235 (also listed under WAF_CORRELATION) - Local File Inclusion (LFI) detections: - 164.92.103.174 (three events) - Network activity: two separate network-communication entries observed Notes for Batch 1: - Some IPs appear in more than one category (e.g., 198.244.240.20 in both WAF_CORRELATION and SQL_INJECTION; 45.195.7.235 in both WAF_CORRELATION and PROTOCOL_ABUSE). - No explicit compromise is stated; detections indicate access attempts and security-rule triggers that were denied or logged. - The events occur within a very short window with multiple simultaneous detections from different sources. Batch 2 (approximately 08:18:37.509–08:18:37.514 UTC) - Event types observed: LFI, WAF_CORRELATION, PROTOCOL_ABUSE, ACCESS_DENIED. - Time clustering: - Sub-batch 1 at 08:18:37.509277 UTC - Sub-batch 2 at 08:18:37.514282 UTC - Source IPs and counts (by event type): - 164.92.103.174: 5 events (LFI x2, WAF_CORRELATION x2, PROTOCOL_ABUSE x1) - 43.166.1.243: 2 events (PROTOCOL_ABUSE x2) - 167.99.116.143: 1 event (ACCESS_DENIED) - 185.73.130.137: 1 event (ACCESS_DENIED) - 216.244.66.199: 12 events total (WAF_CORRELATION x8, PROTOCOL_ABUSE x4) across both sub-batches - 43.155.73.192: 1 event (ACCESS_DENIED) - 217.216.36.182: 1 event (ACCESS_DENIED) - 103.143.231.246: 1 event (ACCESS_DENIED) - 39.109.116.19: 1 event (ACCESS_DENIED) Notes for Batch 2: - The majority of detections originate from 216.244.66.199, appearing as both WAF_CORRELATION and PROTOCOL_ABUSE across both sub-batches. - Several ACCESS_DENIED events are observed across multiple IPs, indicating blocked attempts in this batch. - No explicit indication of successful access or compromise is stated in these events. Batch 3 (timestamp: 2026-01-31 08:18:37.514282 UTC) Overall across this batch: - The batch contains detections and access events across multiple IPs and categories. All events share the same timestamp. No explicit statement of successful compromise is present in the data. No attribution is made. Event categories and counts (by IP): - 216.244.66.199 - WAF_CORRELATION: 2 - PROTOCOL_ABUSE: 1 - 204.76.203.212 - PROTOCOL_ABUSE: 1 - 79.124.40.174 - WAF_CORRELATION: 2 - RCE: 3 - PROTOCOL_ABUSE: 1 - 195.178.110.108 - ACCESS_DENIED: 12 - Network communications - Four network communications observed (no IPs specified) Notes for Batch 3: - Several detections are associated with 79.124.40.174, including WAF_CORRELATION, RCE, and PROTOCOL_ABUSE. - 195.178.110.108 shows multiple ACCESS_DENIED entries (repeated denials). - 216.244.66.199 shows both WAF_CORRELATION and PROTOCOL_ABUSE entries. - Four network-communication observations are noted but without accompanying IP/source/destination details. - The data does not indicate whether any interactions resulted in a successful compromise. Batch 4 (conservative, no speculation) - Source IP: 195.178.110.108 - Event type: ACCESS_DENIED - Timeframe: 2026-01-31, around 08:18:37.514282 to 08:18:37.524460 UTC - Counts: - 14 separate ACCESS_DENIED events at 08:18:37.514282 - 15 separate ACCESS_DENIED events at 08:18:37.524460 Observations: - All events are ACCESS_DENIED; no successful access events are shown in this batch - Both groups occur in a very short time window (approximately 10.178 milliseconds apart) - Additional context: No other IP addresses or event types are reported in this batch Notes for Batch 4: - The pattern shows rapid, repeated denied attempts from the same IP within a tight window. - No corroborating events from other IPs or categories are reported in this batch. Consolidated observations - A high-density, time-clustered set of detections occurred within a narrow window (~10–15 ms) across four batches, involving a mix of ACCESS_DENIED, WAF_CORRELATION, PROTOCOL_ABUSE, LFI, and, in one case, RCE. - The most geographically or structurally prominent source appears to be 216.244.66.199, contributing multiple WAF_CORRELATION and PROTOCOL_ABUSE events across batch 2 and batch 3. - Repeated ACCESS_DENIED activity is observed from 195.178.110.108 (notably in batches 3 and 4), with multiple rapid denials. - LFI detections are concentrated on 164.92.103.174 in batch 2, with accompanying WAF_CORRELATION and PROTOCOL_ABUSE signals. - A small set of other IPs participate across categories, including 79.124.40.174 (WAF_CORRELATION, RCE, PROTOCOL_ABUSE) and 79.124.40.174 in batch 3; 204.76.203.212 and 204.76.203.212 in batch 3 (PROTOCOL_ABUSE) also appear. - SQL_INJECTION is indicated for 198.244.240.20 (batch 1), alongside WAF_CORRELATION; SQL_INJECTION is not observed elsewhere in the provided data. - Four network-communication observations are reported in batch 2 and batch 3 without IPs; no other network-context details are provided for those entries. - Across all batches, there is no explicit statement of successful compromise. Recommended follow-up (non-speculative) - Correlate these batches with additional logs (web server, application, firewall/WAF, proxy) to assemble context for each event (destination/URL, user agent, protocol, payload indicators). - Verify whether any RCE detections (notably associated with 79.124.40.174 in batch 3) correspond to attempted or successful execution, and identify the asset involved. - Review the repeated ACCESS_DENIED events from 195.178.110.108 (batches 3 and 4) for patterns (frequency, targets, timing) to determine if legitimate access attempts occurred. - Investigate the repeated activity from 79.124.40.174 for signs of sustained probing or exploitation attempts. - Consider IP reputation checks and rule-base validation for the WAF and related controls; monitor for repeat activity from the enumerated IPs. - Correlate with available network-communication entries to determine any lateral or external reach attempts. - Do not attribute activity to any actor without explicit evidence; base conclusions strictly on the logged evidence. No attribution or compromise conclusions are drawn from the provided data. The detections indicate access attempts and security-rule triggers that were denied or logged within a tightly clustered time frame.

2. Chronological Event Timeline

Timestamp (UTC)	Observed Event
2026-01-31 08:18:37.504251+00:00	ACCESS_DENIED detected from 178.16.55.142
2026-01-31 08:18:37.504251+00:00	ACCESS_DENIED detected from 178.16.55.142
2026-01-31 08:18:37.504251+00:00	WAF_CORRELATION detected from 198.244.240.20
2026-01-31 08:18:37.504251+00:00	WAF_CORRELATION detected from 198.244.240.20
2026-01-31 08:18:37.504251+00:00	SQL_INJECTION detected from 198.244.240.20
2026-01-31 08:18:37.504251+00:00	Network communication observed
2026-01-31 08:18:37.504251+00:00	PROTOCOL_ABUSE detected from 204.76.203.212
2026-01-31 08:18:37.504251+00:00	WAF_CORRELATION detected from 45.195.7.235
2026-01-31 08:18:37.504251+00:00	WAF_CORRELATION detected from 45.195.7.235
2026-01-31 08:18:37.504251+00:00	PROTOCOL_ABUSE detected from 45.195.7.235
2026-01-31 08:18:37.504251+00:00	Network communication observed
2026-01-31 08:18:37.504251+00:00	ACCESS_DENIED detected from 109.234.161.199
2026-01-31 08:18:37.504251+00:00	ACCESS_DENIED detected from 77.55.253.213
2026-01-31 08:18:37.504251+00:00	ACCESS_DENIED detected from 103.191.208.118
2026-01-31 08:18:37.504251+00:00	ACCESS_DENIED detected from 198.54.126.38
2026-01-31 08:18:37.504251+00:00	ACCESS_DENIED detected from 212.154.119.3
2026-01-31 08:18:37.504251+00:00	ACCESS_DENIED detected from 185.73.130.137
2026-01-31 08:18:37.504251+00:00	ACCESS_DENIED detected from 212.154.119.3
2026-01-31 08:18:37.504251+00:00	ACCESS_DENIED detected from 162.55.240.80
2026-01-31 08:18:37.504251+00:00	ACCESS_DENIED detected from 143.95.111.157
2026-01-31 08:18:37.504251+00:00	ACCESS_DENIED detected from 178.128.239.177
2026-01-31 08:18:37.504251+00:00	ACCESS_DENIED detected from 103.2.225.70
2026-01-31 08:18:37.509277+00:00	LFI detected from 164.92.103.174
2026-01-31 08:18:37.509277+00:00	LFI detected from 164.92.103.174
2026-01-31 08:18:37.509277+00:00	LFI detected from 164.92.103.174
2026-01-31 08:18:37.509277+00:00	LFI detected from 164.92.103.174
2026-01-31 08:18:37.509277+00:00	WAF_CORRELATION detected from 164.92.103.174
2026-01-31 08:18:37.509277+00:00	WAF_CORRELATION detected from 164.92.103.174
2026-01-31 08:18:37.509277+00:00	LFI detected from 164.92.103.174
2026-01-31 08:18:37.509277+00:00	PROTOCOL_ABUSE detected from 164.92.103.174
2026-01-31 08:18:37.509277+00:00	PROTOCOL_ABUSE detected from 43.166.1.243
2026-01-31 08:18:37.509277+00:00	PROTOCOL_ABUSE detected from 43.166.1.243
2026-01-31 08:18:37.509277+00:00	ACCESS_DENIED detected from 167.99.116.143
2026-01-31 08:18:37.509277+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-31 08:18:37.509277+00:00	ACCESS_DENIED detected from 185.73.130.137

Timestamp (UTC)	Observed Event
2026-01-31 08:18:37.509277+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-31 08:18:37.509277+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-31 08:18:37.509277+00:00	ACCESS_DENIED detected from 43.155.73.192
2026-01-31 08:18:37.509277+00:00	ACCESS_DENIED detected from 217.216.36.182
2026-01-31 08:18:37.509277+00:00	ACCESS_DENIED detected from 103.143.231.246
2026-01-31 08:18:37.509277+00:00	ACCESS_DENIED detected from 39.109.116.19
2026-01-31 08:18:37.509277+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-31 08:18:37.509277+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-31 08:18:37.514282+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-31 08:18:37.514282+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-31 08:18:37.514282+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-31 08:18:37.514282+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-31 08:18:37.514282+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-31 08:18:37.514282+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-31 08:18:37.514282+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-31 08:18:37.514282+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-31 08:18:37.514282+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-31 08:18:37.514282+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-31 08:18:37.514282+00:00	PROTOCOL_ABUSE detected from 204.76.203.212
2026-01-31 08:18:37.514282+00:00	Network communication observed
2026-01-31 08:18:37.514282+00:00	Network communication observed
2026-01-31 08:18:37.514282+00:00	Network communication observed
2026-01-31 08:18:37.514282+00:00	Network communication observed
2026-01-31 08:18:37.514282+00:00	WAF_CORRELATION detected from 79.124.40.174
2026-01-31 08:18:37.514282+00:00	WAF_CORRELATION detected from 79.124.40.174
2026-01-31 08:18:37.514282+00:00	RCE detected from 79.124.40.174
2026-01-31 08:18:37.514282+00:00	RCE detected from 79.124.40.174
2026-01-31 08:18:37.514282+00:00	RCE detected from 79.124.40.174
2026-01-31 08:18:37.514282+00:00	PROTOCOL_ABUSE detected from 79.124.40.174
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108

Timestamp (UTC)	Observed Event
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.514282+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.524460+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.524460+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.524460+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.524460+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.524460+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.524460+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.524460+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.524460+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.524460+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.524460+00:00	ACCESS_DENIED detected from 195.178.110.108
2026-01-31 08:18:37.524460+00:00	ACCESS_DENIED detected from 195.178.110.108

3. MITRE ATT&CK; Technique Mapping

Artifact ID	Technique ID	Technique Description
f6c6c09f	T1110	Brute Force / Credential Access
cd182296	T1110	Brute Force / Credential Access
b4c85df8	T1046	Network Service Discovery
f80296ec	T1046	Network Service Discovery
fbd6e8a0	T1190	Exploit Public-Facing Application
3332c4ca	T1048	Exfiltration Over Alternative Protocol
95caa305	T1046	Network Service Discovery
ee5df48e	T1046	Network Service Discovery
1106655b	T1048	Exfiltration Over Alternative Protocol
93e3cc96	T1110	Brute Force / Credential Access
fee9af9d	T1110	Brute Force / Credential Access
114b4e7e	T1110	Brute Force / Credential Access
b1897294	T1110	Brute Force / Credential Access
5b95e70a	T1110	Brute Force / Credential Access
26d6bc20	T1110	Brute Force / Credential Access
9e8aeb41	T1110	Brute Force / Credential Access
9042509b	T1110	Brute Force / Credential Access
e6b628cd	T1110	Brute Force / Credential Access
346c6f37	T1110	Brute Force / Credential Access
fb17d773	T1110	Brute Force / Credential Access
6cd2f917	T1005	Data from Local System
4659d5f9	T1005	Data from Local System
6504aead	T1005	Data from Local System
aa3a8e6e	T1005	Data from Local System
5e002108	T1046	Network Service Discovery
e5ad321e	T1046	Network Service Discovery
ffefcd2b	T1005	Data from Local System
59efa81e	T1048	Exfiltration Over Alternative Protocol
ee4aa389	T1048	Exfiltration Over Alternative Protocol
cfa3f7a9	T1048	Exfiltration Over Alternative Protocol
b618056e	T1110	Brute Force / Credential Access
387d012a	T1046	Network Service Discovery
35f811d9	T1110	Brute Force / Credential Access
3ac09269	T1046	Network Service Discovery
9f2cab42	T1048	Exfiltration Over Alternative Protocol

Artifact ID	Technique ID	Technique Description
455d161c	T1110	Brute Force / Credential Access
3e250f0e	T1110	Brute Force / Credential Access
08bcf173	T1110	Brute Force / Credential Access
9382e8b1	T1110	Brute Force / Credential Access
58936454	T1046	Network Service Discovery
31d537ac	T1046	Network Service Discovery
ffd26b30	T1048	Exfiltration Over Alternative Protocol
fbf028ba	T1046	Network Service Discovery
be69d175	T1046	Network Service Discovery
0834c43d	T1048	Exfiltration Over Alternative Protocol
299dccc4	T1046	Network Service Discovery
aa69e694	T1046	Network Service Discovery
6d7c9b9f	T1048	Exfiltration Over Alternative Protocol
5363f50f	T1046	Network Service Discovery
a53189f1	T1046	Network Service Discovery
02453a8c	T1048	Exfiltration Over Alternative Protocol
4991e812	T1048	Exfiltration Over Alternative Protocol
7a968dd5	T1046	Network Service Discovery
20ab1c4d	T1046	Network Service Discovery
b624f2f2	T1048	Exfiltration Over Alternative Protocol
87a05cf9	T1110	Brute Force / Credential Access
bfc04e05	T1110	Brute Force / Credential Access
cc6f7dee	T1110	Brute Force / Credential Access
760eba6d	T1110	Brute Force / Credential Access
400d51b0	T1110	Brute Force / Credential Access
8a6fef74	T1110	Brute Force / Credential Access
17a879dd	T1110	Brute Force / Credential Access
fce6f995	T1110	Brute Force / Credential Access
82f0ea1d	T1110	Brute Force / Credential Access
7585c31c	T1110	Brute Force / Credential Access
7f890cd2	T1110	Brute Force / Credential Access
de6ace6e	T1110	Brute Force / Credential Access
c45067ef	T1110	Brute Force / Credential Access
7b3a581e	T1110	Brute Force / Credential Access
f78c0b22	T1110	Brute Force / Credential Access
a7464c31	T1110	Brute Force / Credential Access
11fe6fd4	T1110	Brute Force / Credential Access

Artifact ID	Technique ID	Technique Description
ea677979	T1110	Brute Force / Credential Access
1e2eb437	T1110	Brute Force / Credential Access
d9a49e0f	T1110	Brute Force / Credential Access
62b6668b	T1110	Brute Force / Credential Access
c6ade3c5	T1110	Brute Force / Credential Access
09259504	T1110	Brute Force / Credential Access
e1168fb8	T1110	Brute Force / Credential Access
2630d5cd	T1110	Brute Force / Credential Access
14d0a2ef	T1110	Brute Force / Credential Access
1d400b0c	T1110	Brute Force / Credential Access
4a0cbe4d	T1110	Brute Force / Credential Access
7518c54c	T1110	Brute Force / Credential Access
c8fec5da	T1110	Brute Force / Credential Access
e6c50e43	T1110	Brute Force / Credential Access
7b100489	T1110	Brute Force / Credential Access
bd248f70	T1110	Brute Force / Credential Access
3569adc5	T1110	Brute Force / Credential Access
30c5929a	T1110	Brute Force / Credential Access
5b6c0592	T1110	Brute Force / Credential Access

4. Source IP Concentration Analysis

Source IP	Event Count
195.178.110.108	36
216.244.66.199	15
164.92.103.174	8
79.124.40.174	6
178.20.210.148	4
198.244.240.20	3
45.195.7.235	3
178.16.55.142	2
204.76.203.212	2
212.154.119.3	2
185.73.130.137	2
43.166.1.243	2
44.233.146.111	1
195.178.110.68	1
109.234.161.199	1
77.55.253.213	1
103.191.208.118	1
198.54.126.38	1
162.55.240.80	1
143.95.111.157	1
178.128.239.177	1
103.2.225.70	1
167.99.116.143	1
43.155.73.192	1
217.216.36.182	1
103.143.231.246	1
39.109.116.19	1

5. Case Intelligence Summary

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