Digital Forensic Incident Report

Case ID: feac2a9f

Generated: 2026-01-25 09:12:49 UTC

1. Executive Summary

During 09:10:36 UTC on 2026-01-25, a rapid burst of external access attempts was observed. The activity is documented across two batches and is characterized by denied access attempts, with associated security signals. No explicit successful access, data exposure, or confirmation of internal compromise is indicated in either batch. Attribution or actor-specific inference should not be drawn from these logs. Batch 1 — Conservative forensic summary Overview - A rapid spike of external access attempts occurred within a single second around 09:10:36 UTC. - All events are labeled ACCESS_DENIED or related security signals; no success events or breach confirmation are present in this batch. - A small set of external IPs are associated with WAF and protocol-abuse indicators; one generic "Network communication observed" event is noted. - No attribution or actor-specific inference should be made from these logs. Event counts (batch 1) - ACCESS_DENIED: 18 - 103.228.36.130: 2 - 193.202.110.20: 2 - 185.200.240.65: 2 - 152.32.235.239: 2 - 203.209.190.130: 3 - 216.70.80.191: 2 - 34.30.170.78: 3 - 148.66.157.16: 2 - WAF_CORRELATION: 2 - 130.12.180.122: 2 - PROTOCOL_ABUSE: 3 - 130.12.180.122: 1 - 65.49.1.182: 1 - 162.62.213.165: 1 - NETWORK: 1 - "Network communication observed" (no IP) Notable IPs and patterns - Multiple external IPs produced DENIED results within the same second. - 130.12.180.122 exhibits both WAF_CORRELATION (twice) and PROTOCOL_ABUSE (once) within this window. - 34.30.170.78 accounts for three DENIED entries in this window. - 148.66.157.16 accounts for two DENIED entries late in the window. Timeline snapshot (high level) - 09:10:36.117873–09:10:36.118870: Several ACCESS_DENIED events from multiple distinct external sources. - 09:10:36.119870–09:10:36.120868: Additional ACCESS_DENIED events from additional IPs; WAF_CORRELATION signals noted for 130.12.180.122. - 09:10:36.121868–09:10:36.122867: PROTOCOL_ABUSE from 130.12.180.122; NETWORK observation logged. - 09:10:36.122867–09:10:36.123866: PROTOCOL_ABUSE from 65.49.1.182 and additional ACCESS_DENIEDs; PROTOCOL_ABUSE from 162.62.213.165; an ACCESS_DENIED from 148.66.157.16 (second instance) occurs. - 09:10:36.123866: ACCESS_DENIED from 148.66.157.16 (second occurrence) is recorded. Caveats - Do not infer attacker attribution or confirmed breach from these events. - No explicit successful access, data exposure, or internal compromise is indicated in this batch. - Batch 2 may provide additional context or follow-on events; awaiting batch 2 for a complete review. Batch 2 — Conservative forensic summary Time window - All events occurred within 09:10:36.123866 to 09:10:36.130:863 UTC on 2026-01-25. The events are clustered within approximately 7 milliseconds. Event counts (overall) - ACCESS_DENIED: 15 - WAF_CORRELATION: 6 - PROTOCOL_ABUSE: 3 - RCE: 1 Unique source IPs involved (9 total) - 148.66.157.16 - ACCESS_DENIED: 1 - 149.50.150.145 -

ACCESS_DENIED: 3 - 208.109.188.137 - ACCESS_DENIED: 2 - 185.200.240.65 - ACCESS_DENIED: 3 - 216.244.66.199 - WAF_CORRELATION: 2 - PROTOCOL_ABUSE: 1 - 194.164.127.114 - ACCESS_DENIED: 3 - 198.46.83.201 - ACCESS_DENIED: 3 - 34.176.124.12 - WAF_CORRELATION: 2 - PROTOCOL_ABUSE: 1 - 193.142.147.209 - WAF_CORRELATION: 2 - PROTOCOL_ABUSE: 1 - RCE: 1 Notable observations - ACCESS_DENIED is observed across multiple sources, with several IPs contributing more than one event. - WAF_CORRELATION detections occur from three IPs (216.244.66.199; 34.176.124.12; 193.142.147.209). - PROTOCOL_ABUSE detections occur from three IPs (216.244.66.199; 34.176.124.12; 193.142.147.209). - A single RCE detection is recorded from 193.142.147.209. - No explicit successful access events are present in this batch; all reported access attempts are denied, per-frame. Consolidated observations across both batches - Timeframe: The events span a narrow window around 09:10:36 UTC, with batch 1 covering roughly 09:10:36.117873 to 09:10:36.123866 and batch 2 covering 09:10:36.123866 to 09:10:36.130863, indicating a continuous burst across the boundary at 09:10:36.123866. - Denied access attempts: A total of 33 ACCESS_DENIED events are documented across both batches (18 in batch 1, 15 in batch 2). - Security signals: WAF_CORRELATION appears 8 times across both batches; PROTOCOL_ABUSE appears 6 times; an RCE event is observed once (batch 2). - IP involvement: A set of external IPs contributed to the activity, with several IPs appearing across both batches and others appearing in only one batch. Notable repeated sources include IPs that appear with multiple DENIED entries and those that contribute WAF_CORRELATION and PROTOCOL_ABUSE signals. - No explicit successful access or confirmed internal compromise is indicated in either batch. If you would like, I can extract a chronological log of every event with exact timestamps for deeper review.

2. Chronological Event Timeline

Timestamp (UTC)	Observed Event
2026-01-25 09:10:36.117873+00:00	ACCESS_DENIED detected from 103.228.36.130
2026-01-25 09:10:36.117873+00:00	ACCESS_DENIED detected from 103.228.36.130
2026-01-25 09:10:36.118870+00:00	ACCESS_DENIED detected from 193.202.110.20
2026-01-25 09:10:36.118870+00:00	ACCESS_DENIED detected from 193.202.110.20
2026-01-25 09:10:36.118870+00:00	ACCESS_DENIED detected from 185.200.240.65
2026-01-25 09:10:36.118870+00:00	ACCESS_DENIED detected from 185.200.240.65
2026-01-25 09:10:36.119870+00:00	ACCESS_DENIED detected from 152.32.235.239
2026-01-25 09:10:36.119870+00:00	ACCESS_DENIED detected from 152.32.235.239
2026-01-25 09:10:36.119870+00:00	ACCESS_DENIED detected from 203.209.190.130
2026-01-25 09:10:36.119870+00:00	ACCESS_DENIED detected from 203.209.190.130
2026-01-25 09:10:36.119870+00:00	ACCESS_DENIED detected from 203.209.190.130
2026-01-25 09:10:36.119870+00:00	ACCESS_DENIED detected from 216.70.80.191
2026-01-25 09:10:36.119870+00:00	ACCESS_DENIED detected from 216.70.80.191
2026-01-25 09:10:36.120868+00:00	ACCESS_DENIED detected from 216.70.80.191
2026-01-25 09:10:36.120868+00:00	WAF_CORRELATION detected from 130.12.180.122
2026-01-25 09:10:36.120868+00:00	WAF_CORRELATION detected from 130.12.180.122
2026-01-25 09:10:36.121868+00:00	PROTOCOL_ABUSE detected from 130.12.180.122
2026-01-25 09:10:36.121868+00:00	Network communication observed
2026-01-25 09:10:36.122867+00:00	PROTOCOL_ABUSE detected from 65.49.1.182
2026-01-25 09:10:36.122867+00:00	ACCESS_DENIED detected from 34.30.170.78
2026-01-25 09:10:36.122867+00:00	ACCESS_DENIED detected from 34.30.170.78
2026-01-25 09:10:36.122867+00:00	ACCESS_DENIED detected from 34.30.170.78
2026-01-25 09:10:36.122867+00:00	PROTOCOL_ABUSE detected from 162.62.213.165
2026-01-25 09:10:36.122867+00:00	ACCESS_DENIED detected from 148.66.157.16
2026-01-25 09:10:36.123866+00:00	ACCESS_DENIED detected from 148.66.157.16
2026-01-25 09:10:36.123866+00:00	ACCESS_DENIED detected from 148.66.157.16
2026-01-25 09:10:36.123866+00:00	ACCESS_DENIED detected from 149.50.150.145
2026-01-25 09:10:36.123866+00:00	ACCESS_DENIED detected from 149.50.150.145
2026-01-25 09:10:36.123866+00:00	ACCESS_DENIED detected from 149.50.150.145
2026-01-25 09:10:36.123866+00:00	ACCESS_DENIED detected from 208.109.188.137
2026-01-25 09:10:36.123866+00:00	ACCESS_DENIED detected from 208.109.188.137
2026-01-25 09:10:36.124865+00:00	ACCESS_DENIED detected from 185.200.240.65
2026-01-25 09:10:36.124865+00:00	ACCESS_DENIED detected from 185.200.240.65
2026-01-25 09:10:36.124865+00:00	ACCESS_DENIED detected from 185.200.240.65
2026-01-25 09:10:36.124865+00:00	WAF_CORRELATION detected from 216.244.66.199

Timestamp (UTC)	Observed Event
2026-01-25 09:10:36.124865+00:00	WAF_CORRELATION detected from 216.244.66.199
2026-01-25 09:10:36.125865+00:00	PROTOCOL_ABUSE detected from 216.244.66.199
2026-01-25 09:10:36.125865+00:00	ACCESS_DENIED detected from 194.164.127.114
2026-01-25 09:10:36.125865+00:00	ACCESS_DENIED detected from 194.164.127.114
2026-01-25 09:10:36.125865+00:00	ACCESS_DENIED detected from 194.164.127.114
2026-01-25 09:10:36.125865+00:00	ACCESS_DENIED detected from 198.46.83.201
2026-01-25 09:10:36.125865+00:00	ACCESS_DENIED detected from 198.46.83.201
2026-01-25 09:10:36.126864+00:00	ACCESS_DENIED detected from 198.46.83.201
2026-01-25 09:10:36.128863+00:00	WAF_CORRELATION detected from 34.176.124.12
2026-01-25 09:10:36.129114+00:00	WAF_CORRELATION detected from 34.176.124.12
2026-01-25 09:10:36.129114+00:00	PROTOCOL_ABUSE detected from 34.176.124.12
2026-01-25 09:10:36.129863+00:00	WAF_CORRELATION detected from 193.142.147.209
2026-01-25 09:10:36.129863+00:00	WAF_CORRELATION detected from 193.142.147.209
2026-01-25 09:10:36.129863+00:00	RCE detected from 193.142.147.209
2026-01-25 09:10:36.130863+00:00	PROTOCOL_ABUSE detected from 193.142.147.209

3. MITRE ATT&CK; Technique Mapping

Artifact ID	Technique ID	Technique Description
feac2a9f	T1110	Brute Force / Credential Access
00c4d216	T1110	Brute Force / Credential Access
cc693457	T1110	Brute Force / Credential Access
b05cebed	T1110	Brute Force / Credential Access
5906d2f7	T1110	Brute Force / Credential Access
ffb876f2	T1110	Brute Force / Credential Access
3045e605	T1110	Brute Force / Credential Access
79483154	T1110	Brute Force / Credential Access
60cc848f	T1110	Brute Force / Credential Access
d057cee8	T1110	Brute Force / Credential Access
49c430e6	T1110	Brute Force / Credential Access
2fecc4e6	T1110	Brute Force / Credential Access
e379c55e	T1110	Brute Force / Credential Access
9992d1d5	T1110	Brute Force / Credential Access
07388521	T1046	Network Service Discovery
6086d9e8	T1046	Network Service Discovery
0b6399fe	T1048	Exfiltration Over Alternative Protocol
3233b5bc	T1048	Exfiltration Over Alternative Protocol
f5fdc6a8	T1110	Brute Force / Credential Access
b0fa0df2	T1110	Brute Force / Credential Access
e2374278	T1110	Brute Force / Credential Access
75b5af2f	T1048	Exfiltration Over Alternative Protocol
4232d4cd	T1110	Brute Force / Credential Access
520a42d3	T1110	Brute Force / Credential Access
3efbbbf5	T1110	Brute Force / Credential Access
a9a80702	T1110	Brute Force / Credential Access
b35f6478	T1110	Brute Force / Credential Access
62f01430	T1110	Brute Force / Credential Access
940d0ae7	T1110	Brute Force / Credential Access
6436e318	T1110	Brute Force / Credential Access
3580d2e4	T1110	Brute Force / Credential Access
d080641d	T1110	Brute Force / Credential Access
eef2621b	T1110	Brute Force / Credential Access
0f78dcb5	T1046	Network Service Discovery
24bbd685	T1046	Network Service Discovery

Artifact ID	Technique ID	Technique Description
c1e89166	T1048	Exfiltration Over Alternative Protocol
1c2e682c	T1110	Brute Force / Credential Access
7704c486	T1110	Brute Force / Credential Access
192a7d9a	T1110	Brute Force / Credential Access
5f5ffcbe	T1110	Brute Force / Credential Access
b9461120	T1110	Brute Force / Credential Access
a1b0300c	T1110	Brute Force / Credential Access
2780cdf6	T1046	Network Service Discovery
78d5e598	T1046	Network Service Discovery
3864425f	T1048	Exfiltration Over Alternative Protocol
39f445cb	T1046	Network Service Discovery
c9642011	T1046	Network Service Discovery
6954f9ad	T1048	Exfiltration Over Alternative Protocol

4. Source IP Concentration Analysis

Source IP	Event Count
185.200.240.65	5
130.12.180.122	4
193.142.147.209	4
203.209.190.130	3
216.70.80.191	3
34.30.170.78	3
148.66.157.16	3
149.50.150.145	3
216.244.66.199	3
194.164.127.114	3
198.46.83.201	3
34.176.124.12	3
103.228.36.130	2
193.202.110.20	2
152.32.235.239	2
208.109.188.137	2
65.49.1.182	1
162.62.213.165	1

5. Case Intelligence Summary

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