

Digital Forensic Incident Report

Case ID: 138c3c81

Generated: 2026-01-07 08:24:42 UTC

1. Executive Summary

Incident summary (constrained to provided evidence) - The data shows multiple web security events involving WAF and other detections across numerous source IPs and destinations, including

SQL_INJECTION, PROTOCOL_ABUSE, LFI, and general ACCESS_DENIED attempts, with numerous blocks observed. - Representative artifacts and observed patterns: -

138c3c81-59b1-4de8-a0a1-64e1bab23dbc: WAF_CORRELATION detected from 87.106.120.188; decoded content indicates a network connection to 87.106.120.188 on port 60904. -

9fb10ec-8fce-4cf1-9872-9b2c1219dc2d: SQL_INJECTION detected from 87.106.120.188; decoded content indicates a network connection to 87.106.120.188 on port 60904. -

df27f4f4-4d3a-49ac-b36e-b02379422e50: ACCESS_DENIED detected from 47.52.209.228 to 49374. -

d080427f-8c83-4887-86a2-dbce0ea4db3c: ACCESS_DENIED detected from 82.223.9.21 to 38866. -

e43e35d6-c989-44a9-b384-59505e2c3906: ACCESS_DENIED detected from 82.223.9.21 to 38858. -

c4790f5f-5fc2-4773-bca8-efb9a2652a40: ACCESS_DENIED detected from 82.223.9.21 to 38850. -

3de01bcc-b54a-488f-aae0-0c547a4d8d21: SQL_INJECTION detected from 79.137.33.241; network connection to 79.137.33.241 on port 49006. - 2c53ac03-2a27-4683-9f07-b6ae8f062a52:

WAF_CORRELATION detected from 3.136.197.26; network connection to 3.136.197.26 on port 36348. -

20e400fd-8102-42c7-9284-a067d78bdfe5: SQL_INJECTION detected from 3.136.197.26; network connection to 3.136.197.26 on port 36348. - 3b1e426b-27b6-453a-80a4-09410cbd76c9:

PROTOCOL_ABUSE detected from 149.50.103.48; network connection to 149.50.103.48 on port 47850.

- 0e50831e-23a5-4b68-9a56-0251ca44bcc: LFI detected from 93.123.109.135; network connection to 93.123.109.135 on port 56558. - 93.123.109.135 related artifacts show multiple LFI detections and

WAF_CORRELATION entries with the same port 56558. - 64.62.210.38 and related artifacts (multiple WAF_CORRELATION and PROTOCOL_ABUSE entries) show repeated patterns of correlations and protocol abuse attempts to various ports. - 45.227.162.235 and 174.142.31.70 show

WAF_CORRELATION, PROTOCOL_ABUSE, and SQL_INJECTION detections with corresponding network connections. - 51.38.109.223 and 157.20.32.130 show LFI detections with multiple related artifacts. -

74.176.56.30 and associated artifacts (numerous network_event and web_security_event entries) indicate continued network activity targeting that host, with many entries labeled as NETWORK_COMMUNICATION_OBSERVED and multiple ACCESS_DENIED events. - Additional observations: - A number of entries are labeled as ACCESS_DENIED from various IPs (examples include 82.223.9.21; 47.52.209.228; 194.195.86.82; 220.158.233.50; .ut). This pattern appears across many destinations and ports. - Several SQL_INJECTION detections are paired with WAF_CORRELATION entries from the same source IPs (e.g.,

87.106.120.188; 79.137.33.241; 3.136.197.26; 179.108.84.136; 104.199.79.203; 91.107.124.38; 93.123.109.135), often tied to specific destination ports. - PROTOCOL_ABUSE and LFI detections are present from multiple IPs, sometimes with repeated WAF_CORRELATION indicators. - No explicit timestamps or success indicators are present beyond the artifact content; the artifacts collectively indicate repeated web security events with various threat detections and block actions across multiple source IPs.

2. Chronological Event Timeline

Timestamp (UTC)	Observed Event
2026-01-07 08:23:45.681274+00:00	WAF_CORRELATION detected from 87.106.120.188
2026-01-07 08:23:45.681422+00:00	SQL_INJECTION detected from 87.106.120.188
2026-01-07 08:23:45.682373+00:00	ACCESS_DENIED detected from 47.52.209.228
2026-01-07 08:23:45.683170+00:00	ACCESS_DENIED detected from 82.223.9.21
2026-01-07 08:23:45.684011+00:00	ACCESS_DENIED detected from 82.223.9.21
2026-01-07 08:23:45.684892+00:00	ACCESS_DENIED detected from 47.52.209.228
2026-01-07 08:23:45.685785+00:00	ACCESS_DENIED detected from 82.223.9.21
2026-01-07 08:23:45.686622+00:00	ACCESS_DENIED detected from 47.52.209.228
2026-01-07 08:23:45.687537+00:00	ACCESS_DENIED detected from 82.223.9.21
2026-01-07 08:23:45.688438+00:00	ACCESS_DENIED detected from 82.223.9.21
2026-01-07 08:23:45.689227+00:00	ACCESS_DENIED detected from 82.223.9.21
2026-01-07 08:23:45.690100+00:00	ACCESS_DENIED detected from 194.195.86.82
2026-01-07 08:23:45.691193+00:00	ACCESS_DENIED detected from 194.195.86.82
2026-01-07 08:23:45.691961+00:00	ACCESS_DENIED detected from 194.195.86.82
2026-01-07 08:23:45.692631+00:00	ACCESS_DENIED detected from 220.158.233.50
2026-01-07 08:23:45.693384+00:00	ACCESS_DENIED detected from 220.158.233.50
2026-01-07 08:23:45.694007+00:00	ACCESS_DENIED detected from 220.158.233.50
2026-01-07 08:23:45.694430+00:00	ACCESS_DENIED detected from 80.88.86.96
2026-01-07 08:23:45.694816+00:00	ACCESS_DENIED detected from 80.88.86.96
2026-01-07 08:23:45.695293+00:00	ACCESS_DENIED detected from 80.88.86.96
2026-01-07 08:23:45.696103+00:00	ACCESS_DENIED detected from 212.52.28.106
2026-01-07 08:23:45.696560+00:00	ACCESS_DENIED detected from 212.52.28.106
2026-01-07 08:23:45.696927+00:00	ACCESS_DENIED detected from 212.52.28.106
2026-01-07 08:23:45.697520+00:00	ACCESS_DENIED detected from 185.187.75.18
2026-01-07 08:23:45.698062+00:00	ACCESS_DENIED detected from 185.187.75.18
2026-01-07 08:23:45.698505+00:00	ACCESS_DENIED detected from 185.187.75.18
2026-01-07 08:23:45.698880+00:00	ACCESS_DENIED detected from 197.189.255.202
2026-01-07 08:23:45.699621+00:00	ACCESS_DENIED detected from 197.189.255.202
2026-01-07 08:23:45.700001+00:00	ACCESS_DENIED detected from 197.189.255.202
2026-01-07 08:23:45.700498+00:00	ACCESS_DENIED detected from 212.52.28.106
2026-01-07 08:23:45.700867+00:00	ACCESS_DENIED detected from 212.52.28.106
2026-01-07 08:23:45.701427+00:00	ACCESS_DENIED detected from 212.52.28.106
2026-01-07 08:23:45.701864+00:00	ACCESS_DENIED detected from 103.168.21.194
2026-01-07 08:23:45.702222+00:00	ACCESS_DENIED detected from 103.168.21.194
2026-01-07 08:23:45.702625+00:00	ACCESS_DENIED detected from 103.168.21.194

Timestamp (UTC)	Observed Event
2026-01-07 08:23:45.702976+00:00	ACCESS_DENIED detected from 103.168.21.194
2026-01-07 08:23:45.703454+00:00	ACCESS_DENIED detected from 103.168.21.194
2026-01-07 08:23:45.703820+00:00	ACCESS_DENIED detected from 103.168.21.194
2026-01-07 08:23:45.704542+00:00	PROTOCOL_ABUSE detected from 95.214.55.71
2026-01-07 08:23:45.706275+00:00	Network communication observed
2026-01-07 08:23:45.707123+00:00	WAF_CORRELATION detected from 79.137.33.241
2026-01-07 08:23:45.707950+00:00	WAF_CORRELATION detected from 79.137.33.241
2026-01-07 08:23:45.708030+00:00	SQL_INJECTION detected from 79.137.33.241
2026-01-07 08:23:45.708933+00:00	WAF_CORRELATION detected from 3.136.197.26
2026-01-07 08:23:45.710182+00:00	WAF_CORRELATION detected from 3.136.197.26
2026-01-07 08:23:45.710335+00:00	SQL_INJECTION detected from 3.136.197.26
2026-01-07 08:23:45.711020+00:00	Network communication observed
2026-01-07 08:23:45.711347+00:00	ACCESS_DENIED detected from 74.234.147.76
2026-01-07 08:23:45.711665+00:00	ACCESS_DENIED detected from 74.234.147.76
2026-01-07 08:23:45.711945+00:00	ACCESS_DENIED detected from 74.234.147.76
2026-01-07 08:23:45.712068+00:00	ACCESS_DENIED detected from 74.234.147.76
2026-01-07 08:23:45.712291+00:00	ACCESS_DENIED detected from 74.234.147.76
2026-01-07 08:23:45.712498+00:00	ACCESS_DENIED detected from 74.234.147.76
2026-01-07 08:23:45.712994+00:00	PROTOCOL_ABUSE detected from 149.50.103.48
2026-01-07 08:23:45.713268+00:00	Network communication observed
2026-01-07 08:23:45.713564+00:00	Network communication observed
2026-01-07 08:23:45.713740+00:00	ACCESS_DENIED detected from 128.65.195.33
2026-01-07 08:23:45.713863+00:00	ACCESS_DENIED detected from 128.65.195.33
2026-01-07 08:23:45.713960+00:00	ACCESS_DENIED detected from 128.65.195.33
2026-01-07 08:23:45.714064+00:00	ACCESS_DENIED detected from 128.65.195.33
2026-01-07 08:23:45.714148+00:00	ACCESS_DENIED detected from 128.65.195.33
2026-01-07 08:23:45.714299+00:00	ACCESS_DENIED detected from 20.184.35.52
2026-01-07 08:23:45.714408+00:00	ACCESS_DENIED detected from 20.184.35.52
2026-01-07 08:23:45.714508+00:00	ACCESS_DENIED detected from 20.184.35.52
2026-01-07 08:23:45.714592+00:00	ACCESS_DENIED detected from 128.65.195.33
2026-01-07 08:23:45.714684+00:00	Network communication observed
2026-01-07 08:23:45.714859+00:00	PROTOCOL_ABUSE detected from 204.76.203.212
2026-01-07 08:23:45.714947+00:00	Network communication observed
2026-01-07 08:23:45.715089+00:00	Network communication observed
2026-01-07 08:23:45.715326+00:00	WAF_CORRELATION detected from 207.38.87.177
2026-01-07 08:23:45.715521+00:00	WAF_CORRELATION detected from 207.38.87.177
2026-01-07 08:23:45.715541+00:00	SQL_INJECTION detected from 207.38.87.177

Timestamp (UTC)	Observed Event
2026-01-07 08:23:45.715648+00:00	Network communication observed
2026-01-07 08:23:45.715885+00:00	WAF_CORRELATION detected from 15.235.203.43
2026-01-07 08:23:45.716182+00:00	WAF_CORRELATION detected from 15.235.203.43
2026-01-07 08:23:45.716210+00:00	SQL_INJECTION detected from 15.235.203.43
2026-01-07 08:23:45.716343+00:00	ACCESS_DENIED detected from 20.184.35.52
2026-01-07 08:23:45.716871+00:00	Network communication observed
2026-01-07 08:23:45.717123+00:00	WAF_CORRELATION detected from 179.108.84.136
2026-01-07 08:23:45.717370+00:00	WAF_CORRELATION detected from 179.108.84.136
2026-01-07 08:23:45.717399+00:00	SQL_INJECTION detected from 179.108.84.136
2026-01-07 08:23:45.717688+00:00	PROTOCOL_ABUSE detected from 43.140.247.223
2026-01-07 08:23:45.717865+00:00	ACCESS_DENIED detected from 91.204.46.136
2026-01-07 08:23:45.718048+00:00	ACCESS_DENIED detected from 91.204.46.136
2026-01-07 08:23:45.718202+00:00	ACCESS_DENIED detected from 91.204.46.136
2026-01-07 08:23:45.718603+00:00	PROTOCOL_ABUSE detected from 43.140.247.223
2026-01-07 08:23:45.718814+00:00	ACCESS_DENIED detected from 91.204.46.136
2026-01-07 08:23:45.719058+00:00	ACCESS_DENIED detected from 91.204.46.136
2026-01-07 08:23:45.719287+00:00	ACCESS_DENIED detected from 91.204.46.136
2026-01-07 08:23:45.719743+00:00	WAF_CORRELATION detected from 104.199.79.203
2026-01-07 08:23:45.720028+00:00	WAF_CORRELATION detected from 104.199.79.203
2026-01-07 08:23:45.720051+00:00	SQL_INJECTION detected from 104.199.79.203
2026-01-07 08:23:45.720283+00:00	WAF_CORRELATION detected from 20.163.78.59
2026-01-07 08:23:45.720489+00:00	WAF_CORRELATION detected from 20.163.78.59
2026-01-07 08:23:45.720738+00:00	Network communication observed
2026-01-07 08:23:45.720994+00:00	Network communication observed
2026-01-07 08:23:45.721258+00:00	Network communication observed
2026-01-07 08:23:45.721523+00:00	Network communication observed
2026-01-07 08:23:45.721713+00:00	PROTOCOL_ABUSE detected from 176.65.148.177
2026-01-07 08:23:45.721770+00:00	Network communication observed
2026-01-07 08:23:45.721825+00:00	Network communication observed
2026-01-07 08:23:45.721879+00:00	Network communication observed
2026-01-07 08:23:45.721932+00:00	Network communication observed
2026-01-07 08:23:45.721990+00:00	Network communication observed
2026-01-07 08:23:45.722046+00:00	Network communication observed
2026-01-07 08:23:45.722214+00:00	PROTOCOL_ABUSE detected from 147.185.132.234
2026-01-07 08:23:45.722303+00:00	Network communication observed
2026-01-07 08:23:45.722358+00:00	Network communication observed
2026-01-07 08:23:45.722411+00:00	Network communication observed

Timestamp (UTC)	Observed Event
2026-01-07 08:23:45.722464+00:00	Network communication observed
2026-01-07 08:23:45.722517+00:00	Network communication observed
2026-01-07 08:23:45.722570+00:00	Network communication observed
2026-01-07 08:23:45.722627+00:00	Network communication observed
2026-01-07 08:23:45.722685+00:00	Network communication observed
2026-01-07 08:23:45.722738+00:00	Network communication observed
2026-01-07 08:23:45.722791+00:00	Network communication observed
2026-01-07 08:23:45.722844+00:00	Network communication observed
2026-01-07 08:23:45.722897+00:00	Network communication observed
2026-01-07 08:23:45.722950+00:00	Network communication observed
2026-01-07 08:23:45.723006+00:00	Network communication observed
2026-01-07 08:23:45.723061+00:00	Network communication observed
2026-01-07 08:23:45.723114+00:00	Network communication observed
2026-01-07 08:23:45.723184+00:00	Network communication observed
2026-01-07 08:23:45.723262+00:00	Network communication observed
2026-01-07 08:23:45.723328+00:00	Network communication observed
2026-01-07 08:23:45.723383+00:00	Network communication observed
2026-01-07 08:23:45.723437+00:00	Network communication observed
2026-01-07 08:23:45.723490+00:00	Network communication observed
2026-01-07 08:23:45.723543+00:00	Network communication observed
2026-01-07 08:23:45.723610+00:00	Network communication observed
2026-01-07 08:23:45.723673+00:00	Network communication observed
2026-01-07 08:23:45.723725+00:00	Network communication observed
2026-01-07 08:23:45.723777+00:00	Network communication observed
2026-01-07 08:23:45.723834+00:00	Network communication observed
2026-01-07 08:23:45.723886+00:00	Network communication observed
2026-01-07 08:23:45.723950+00:00	Network communication observed
2026-01-07 08:23:45.724003+00:00	Network communication observed
2026-01-07 08:23:45.724056+00:00	Network communication observed
2026-01-07 08:23:45.724109+00:00	Network communication observed
2026-01-07 08:23:45.724162+00:00	Network communication observed
2026-01-07 08:23:45.724215+00:00	Network communication observed
2026-01-07 08:23:45.724296+00:00	Network communication observed
2026-01-07 08:23:45.724349+00:00	Network communication observed
2026-01-07 08:23:45.724405+00:00	Network communication observed
2026-01-07 08:23:45.724458+00:00	Network communication observed
2026-01-07 08:23:45.724511+00:00	Network communication observed

Timestamp (UTC)	Observed Event
2026-01-07 08:23:45.724566+00:00	Network communication observed
2026-01-07 08:23:45.724619+00:00	Network communication observed
2026-01-07 08:23:45.724672+00:00	Network communication observed
2026-01-07 08:23:45.724725+00:00	Network communication observed
2026-01-07 08:23:45.724778+00:00	Network communication observed
2026-01-07 08:23:45.724833+00:00	Network communication observed
2026-01-07 08:23:45.724886+00:00	Network communication observed
2026-01-07 08:23:45.724942+00:00	Network communication observed
2026-01-07 08:23:45.724994+00:00	Network communication observed
2026-01-07 08:23:45.725047+00:00	Network communication observed
2026-01-07 08:23:45.725099+00:00	Network communication observed
2026-01-07 08:23:45.725155+00:00	Network communication observed
2026-01-07 08:23:45.725208+00:00	Network communication observed
2026-01-07 08:23:45.725287+00:00	Network communication observed
2026-01-07 08:23:45.725340+00:00	Network communication observed
2026-01-07 08:23:45.725392+00:00	Network communication observed
2026-01-07 08:23:45.725444+00:00	Network communication observed
2026-01-07 08:23:45.725499+00:00	Network communication observed
2026-01-07 08:23:45.725552+00:00	Network communication observed
2026-01-07 08:23:45.725604+00:00	Network communication observed
2026-01-07 08:23:45.725660+00:00	Network communication observed
2026-01-07 08:23:45.725738+00:00	Network communication observed
2026-01-07 08:23:45.725791+00:00	Network communication observed
2026-01-07 08:23:45.725846+00:00	Network communication observed
2026-01-07 08:23:45.725899+00:00	Network communication observed
2026-01-07 08:23:45.725952+00:00	Network communication observed
2026-01-07 08:23:45.726005+00:00	Network communication observed
2026-01-07 08:23:45.726095+00:00	ACCESS_DENIED detected from 45.56.222.60
2026-01-07 08:23:45.726181+00:00	ACCESS_DENIED detected from 45.56.222.60
2026-01-07 08:23:45.726270+00:00	ACCESS_DENIED detected from 45.56.222.60
2026-01-07 08:23:45.726355+00:00	ACCESS_DENIED detected from 45.56.222.60
2026-01-07 08:23:45.726439+00:00	ACCESS_DENIED detected from 45.56.222.60
2026-01-07 08:23:45.726527+00:00	ACCESS_DENIED detected from 45.56.222.60
2026-01-07 08:23:45.726626+00:00	ACCESS_DENIED detected from 121.127.34.151
2026-01-07 08:23:45.726793+00:00	PROTOCOL_ABUSE detected from 204.76.203.212
2026-01-07 08:23:45.727005+00:00	WAF_CORRELATION detected from 91.107.124.38
2026-01-07 08:23:45.727198+00:00	WAF_CORRELATION detected from 91.107.124.38

Timestamp (UTC)	Observed Event
2026-01-07 08:23:45.727223+00:00	SQL_INJECTION detected from 91.107.124.38
2026-01-07 08:23:45.727322+00:00	ACCESS_DENIED detected from 157.20.32.130
2026-01-07 08:23:45.727421+00:00	ACCESS_DENIED detected from 157.20.32.130
2026-01-07 08:23:45.727517+00:00	Network communication observed
2026-01-07 08:23:45.727609+00:00	ACCESS_DENIED detected from 157.20.32.130
2026-01-07 08:23:45.727667+00:00	Network communication observed
2026-01-07 08:23:45.727722+00:00	Network communication observed
2026-01-07 08:23:45.727818+00:00	Network communication observed
2026-01-07 08:23:45.727873+00:00	Network communication observed
2026-01-07 08:23:45.727925+00:00	Network communication observed
2026-01-07 08:23:45.728029+00:00	Network communication observed
2026-01-07 08:23:45.728155+00:00	Network communication observed
2026-01-07 08:23:45.728262+00:00	Network communication observed
2026-01-07 08:23:45.728359+00:00	ACCESS_DENIED detected from 222.252.11.23
2026-01-07 08:23:45.728444+00:00	ACCESS_DENIED detected from 118.70.190.36
2026-01-07 08:23:45.728533+00:00	ACCESS_DENIED detected from 222.252.11.23
2026-01-07 08:23:45.728620+00:00	ACCESS_DENIED detected from 118.70.190.36
2026-01-07 08:23:45.728703+00:00	ACCESS_DENIED detected from 222.252.11.23
2026-01-07 08:23:45.728787+00:00	ACCESS_DENIED detected from 222.252.11.133
2026-01-07 08:23:45.728871+00:00	ACCESS_DENIED detected from 160.191.139.216
2026-01-07 08:23:45.728956+00:00	ACCESS_DENIED detected from 160.191.139.216
2026-01-07 08:23:45.729053+00:00	ACCESS_DENIED detected from 160.191.139.216
2026-01-07 08:23:45.729151+00:00	ACCESS_DENIED detected from 160.191.139.216
2026-01-07 08:23:45.729250+00:00	ACCESS_DENIED detected from 160.191.139.216
2026-01-07 08:23:45.729348+00:00	ACCESS_DENIED detected from 160.191.139.216
2026-01-07 08:23:45.729446+00:00	ACCESS_DENIED detected from 81.88.49.27
2026-01-07 08:23:45.729531+00:00	ACCESS_DENIED detected from 81.88.49.27
2026-01-07 08:23:45.729614+00:00	ACCESS_DENIED detected from 81.88.49.27
2026-01-07 08:23:45.729696+00:00	ACCESS_DENIED detected from 81.88.49.27
2026-01-07 08:23:45.729790+00:00	ACCESS_DENIED detected from 81.88.49.27
2026-01-07 08:23:45.729882+00:00	ACCESS_DENIED detected from 81.88.49.27
2026-01-07 08:23:45.730081+00:00	WAF_CORRELATION detected from 173.199.123.6
2026-01-07 08:23:45.730304+00:00	WAF_CORRELATION detected from 173.199.123.6
2026-01-07 08:23:45.730323+00:00	SQL_INJECTION detected from 173.199.123.6
2026-01-07 08:23:45.730485+00:00	PROTOCOL_ABUSE detected from 204.76.203.18
2026-01-07 08:23:45.730675+00:00	PROTOCOL_ABUSE detected from 154.82.150.126
2026-01-07 08:23:45.730873+00:00	PROTOCOL_ABUSE detected from 154.82.171.11

Timestamp (UTC)	Observed Event
2026-01-07 08:23:45.731063+00:00	PROTOCOL_ABUSE detected from 156.239.204.135
2026-01-07 08:23:45.731273+00:00	PROTOCOL_ABUSE detected from 154.82.169.248
2026-01-07 08:23:45.731474+00:00	PROTOCOL_ABUSE detected from 156.239.206.170
2026-01-07 08:23:45.731613+00:00	LFI detected from 51.38.109.223
2026-01-07 08:23:45.731781+00:00	LFI detected from 51.38.109.223
2026-01-07 08:23:45.731947+00:00	LFI detected from 51.38.109.223
2026-01-07 08:23:45.732153+00:00	WAF_CORRELATION detected from 41.90.64.136
2026-01-07 08:23:45.732386+00:00	WAF_CORRELATION detected from 41.90.64.136
2026-01-07 08:23:45.732634+00:00	PROTOCOL_ABUSE detected from 41.90.64.136
2026-01-07 08:23:45.732730+00:00	ACCESS_DENIED detected from 66.240.223.230
2026-01-07 08:23:45.732841+00:00	ACCESS_DENIED detected from 66.240.223.230
2026-01-07 08:23:45.732925+00:00	ACCESS_DENIED detected from 66.240.223.230
2026-01-07 08:23:45.733008+00:00	ACCESS_DENIED detected from 66.240.223.230
2026-01-07 08:23:45.733092+00:00	ACCESS_DENIED detected from 66.240.223.230
2026-01-07 08:23:45.733176+00:00	ACCESS_DENIED detected from 66.240.223.230
2026-01-07 08:23:45.733312+00:00	LFI detected from 157.20.32.130
2026-01-07 08:23:45.733415+00:00	LFI detected from 157.20.32.130
2026-01-07 08:23:45.733510+00:00	LFI detected from 157.20.32.130
2026-01-07 08:23:45.733614+00:00	LFI detected from 157.20.32.130
2026-01-07 08:23:45.733738+00:00	LFI detected from 157.20.32.130
2026-01-07 08:23:45.733845+00:00	LFI detected from 157.20.32.130
2026-01-07 08:23:45.733941+00:00	ACCESS_DENIED detected from 174.142.31.70
2026-01-07 08:23:45.734024+00:00	ACCESS_DENIED detected from 174.142.31.70
2026-01-07 08:23:45.734107+00:00	ACCESS_DENIED detected from 174.142.31.70
2026-01-07 08:23:45.734326+00:00	WAF_CORRELATION detected from 45.227.162.235
2026-01-07 08:23:45.734410+00:00	ACCESS_DENIED detected from 174.142.31.70
2026-01-07 08:23:45.734601+00:00	WAF_CORRELATION detected from 45.227.162.235
2026-01-07 08:23:45.734618+00:00	SQL_INJECTION detected from 45.227.162.235
2026-01-07 08:23:45.734701+00:00	ACCESS_DENIED detected from 174.142.31.70
2026-01-07 08:23:45.734788+00:00	ACCESS_DENIED detected from 174.142.31.70
2026-01-07 08:23:45.734913+00:00	LFI detected from 157.20.32.130
2026-01-07 08:23:45.735030+00:00	LFI detected from 157.20.32.130
2026-01-07 08:23:45.735197+00:00	LFI detected from 157.20.32.130
2026-01-07 08:23:45.735438+00:00	LFI detected from 157.20.32.130
2026-01-07 08:23:45.735568+00:00	LFI detected from 157.20.32.130
2026-01-07 08:23:45.735681+00:00	LFI detected from 157.20.32.130
2026-01-07 08:23:45.735770+00:00	ACCESS_DENIED detected from 194.195.245.44

Timestamp (UTC)	Observed Event
2026-01-07 08:23:45.735856+00:00	ACCESS_DENIED detected from 194.195.245.44
2026-01-07 08:23:45.735941+00:00	ACCESS_DENIED detected from 194.195.245.44
2026-01-07 08:23:45.736029+00:00	ACCESS_DENIED detected from 194.195.245.44
2026-01-07 08:23:45.736114+00:00	ACCESS_DENIED detected from 194.195.245.44
2026-01-07 08:23:45.736297+00:00	Network communication observed
2026-01-07 08:23:45.736393+00:00	ACCESS_DENIED detected from 194.195.245.44
2026-01-07 08:23:45.736579+00:00	PROTOCOL_ABUSE detected from 34.78.138.227
2026-01-07 08:23:45.736786+00:00	WAF_CORRELATION detected from 34.82.67.239
2026-01-07 08:23:45.736979+00:00	WAF_CORRELATION detected from 34.82.67.239
2026-01-07 08:23:45.737183+00:00	PROTOCOL_ABUSE detected from 34.82.67.239
2026-01-07 08:23:45.737397+00:00	WAF_CORRELATION detected from 54.37.118.70
2026-01-07 08:23:45.737577+00:00	WAF_CORRELATION detected from 54.37.118.70
2026-01-07 08:23:45.737620+00:00	SQL_INJECTION detected from 54.37.118.70
2026-01-07 08:23:45.737802+00:00	WAF_CORRELATION detected from 93.123.109.135
2026-01-07 08:23:45.737902+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.738018+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.738128+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.738222+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.738321+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.738424+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.738530+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.738731+00:00	WAF_CORRELATION detected from 93.123.109.135
2026-01-07 08:23:45.738828+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.738927+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.739033+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.739128+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.739259+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.739379+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.739487+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.739696+00:00	WAF_CORRELATION detected from 93.123.109.135
2026-01-07 08:23:45.739789+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.739894+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.740004+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.740204+00:00	WAF_CORRELATION detected from 93.123.109.135
2026-01-07 08:23:45.740304+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.740404+00:00	LFI detected from 93.123.109.135
2026-01-07 08:23:45.740513+00:00	LFI detected from 93.123.109.135

Timestamp (UTC)	Observed Event
2026-01-07 08:23:45.740615+00:00	ACCESS_DENIED detected from 4.190.203.84
2026-01-07 08:23:45.740840+00:00	WAF_CORRELATION detected from 64.62.210.38
2026-01-07 08:23:45.741057+00:00	WAF_CORRELATION detected from 64.62.210.38
2026-01-07 08:23:45.741308+00:00	PROTOCOL_ABUSE detected from 64.62.210.38
2026-01-07 08:23:45.741498+00:00	WAF_CORRELATION detected from 64.62.210.38
2026-01-07 08:23:45.741700+00:00	WAF_CORRELATION detected from 64.62.210.38
2026-01-07 08:23:45.741895+00:00	WAF_CORRELATION detected from 64.62.210.38
2026-01-07 08:23:45.742122+00:00	PROTOCOL_ABUSE detected from 64.62.210.38
2026-01-07 08:23:45.742341+00:00	WAF_CORRELATION detected from 64.62.210.38
2026-01-07 08:23:45.742535+00:00	WAF_CORRELATION detected from 64.62.210.38
2026-01-07 08:23:45.742728+00:00	WAF_CORRELATION detected from 64.62.210.38
2026-01-07 08:23:45.742920+00:00	WAF_CORRELATION detected from 64.62.210.38
2026-01-07 08:23:45.743113+00:00	WAF_CORRELATION detected from 64.62.210.38
2026-01-07 08:23:45.743341+00:00	PROTOCOL_ABUSE detected from 64.62.210.38
2026-01-07 08:23:45.743559+00:00	PROTOCOL_ABUSE detected from 64.62.210.38
2026-01-07 08:23:45.743757+00:00	WAF_CORRELATION detected from 64.62.210.38
2026-01-07 08:23:45.743947+00:00	WAF_CORRELATION detected from 64.62.210.38
2026-01-07 08:23:45.744142+00:00	WAF_CORRELATION detected from 64.62.210.38
2026-01-07 08:23:45.744335+00:00	WAF_CORRELATION detected from 64.62.210.38
2026-01-07 08:23:45.744538+00:00	PROTOCOL_ABUSE detected from 64.62.210.38
2026-01-07 08:23:45.744726+00:00	WAF_CORRELATION detected from 64.62.210.38
2026-01-07 08:23:45.744929+00:00	PROTOCOL_ABUSE detected from 64.62.210.38
2026-01-07 08:23:45.745129+00:00	PROTOCOL_ABUSE detected from 64.62.210.38
2026-01-07 08:23:45.745351+00:00	WAF_CORRELATION detected from 64.62.210.38
2026-01-07 08:23:45.745544+00:00	WAF_CORRELATION detected from 64.62.210.38

3. MITRE ATT&CK; Technique Mapping

Artifact ID	Technique ID	Technique Description
138c3c81	T1046	Network Service Discovery
9fdbd10ec	T1190	Exploit Public-Facing Application
df27f4f4	T1110	Brute Force / Credential Access
d080427f	T1110	Brute Force / Credential Access
e43e35d6	T1110	Brute Force / Credential Access
49f0ec81	T1110	Brute Force / Credential Access
c4790f5f	T1110	Brute Force / Credential Access
76b0e4ba	T1110	Brute Force / Credential Access
9fa709d0	T1110	Brute Force / Credential Access
3581aff0	T1110	Brute Force / Credential Access
f4191415	T1110	Brute Force / Credential Access
bdbb9609	T1110	Brute Force / Credential Access
5f0d5e79	T1110	Brute Force / Credential Access
1db0744f	T1110	Brute Force / Credential Access
36d1438e	T1110	Brute Force / Credential Access
5d6845f9	T1110	Brute Force / Credential Access
c7d909aa	T1110	Brute Force / Credential Access
feecdac7	T1110	Brute Force / Credential Access
f32289b8	T1110	Brute Force / Credential Access
328017e7	T1110	Brute Force / Credential Access
3df15ba6	T1110	Brute Force / Credential Access
6a1064bb	T1110	Brute Force / Credential Access
8e062334	T1110	Brute Force / Credential Access
d04e83c9	T1110	Brute Force / Credential Access
7cadd309	T1110	Brute Force / Credential Access
b86f9141	T1110	Brute Force / Credential Access
3cd1ac16	T1110	Brute Force / Credential Access
718cf230	T1110	Brute Force / Credential Access
cfa87152	T1110	Brute Force / Credential Access
c23073d2	T1110	Brute Force / Credential Access
bdb746c3	T1110	Brute Force / Credential Access
fdb8afdb	T1110	Brute Force / Credential Access
85baa99c	T1110	Brute Force / Credential Access
2f9e64b4	T1110	Brute Force / Credential Access
69e101fa	T1110	Brute Force / Credential Access

Artifact ID	Technique ID	Technique Description
e18e670a	T1110	Brute Force / Credential Access
326fa03e	T1110	Brute Force / Credential Access
d9ac0647	T1110	Brute Force / Credential Access
cf8010c2	T1048	Exfiltration Over Alternative Protocol
419c84c1	T1046	Network Service Discovery
c1f4b13d	T1046	Network Service Discovery
3de01bcc	T1190	Exploit Public-Facing Application
2c53ac03	T1046	Network Service Discovery
51909f1a	T1046	Network Service Discovery
20e400fd	T1190	Exploit Public-Facing Application
066ae55d	T1110	Brute Force / Credential Access
6deb514b	T1110	Brute Force / Credential Access
22482b92	T1110	Brute Force / Credential Access
736ef1c4	T1110	Brute Force / Credential Access
ce630ca1	T1110	Brute Force / Credential Access
6147ffd1	T1110	Brute Force / Credential Access
3b1e426b	T1048	Exfiltration Over Alternative Protocol
d152d9ea	T1110	Brute Force / Credential Access
2dfd4704	T1110	Brute Force / Credential Access
92da5412	T1110	Brute Force / Credential Access
a5a95ea1	T1110	Brute Force / Credential Access
d814aa05	T1110	Brute Force / Credential Access
32c2dea4	T1110	Brute Force / Credential Access
c2bf5ff9	T1110	Brute Force / Credential Access
86f4f2fe	T1110	Brute Force / Credential Access
973848a8	T1110	Brute Force / Credential Access
75574226	T1048	Exfiltration Over Alternative Protocol
c8cc86ce	T1046	Network Service Discovery
96ba2a80	T1046	Network Service Discovery
0afac763	T1190	Exploit Public-Facing Application
1f007f95	T1046	Network Service Discovery
0c4653eb	T1046	Network Service Discovery
596880ed	T1190	Exploit Public-Facing Application
9d020b8a	T1110	Brute Force / Credential Access
234a1405	T1046	Network Service Discovery
9f448e7c	T1046	Network Service Discovery
dc2a0e47	T1190	Exploit Public-Facing Application

Artifact ID	Technique ID	Technique Description
82125854	T1048	Exfiltration Over Alternative Protocol
b435748c	T1110	Brute Force / Credential Access
8d21fcf5	T1110	Brute Force / Credential Access
325c2625	T1110	Brute Force / Credential Access
17bb664f	T1048	Exfiltration Over Alternative Protocol
cffa4ddb	T1110	Brute Force / Credential Access
24a6d848	T1110	Brute Force / Credential Access
d601d74c	T1110	Brute Force / Credential Access
419e298d	T1046	Network Service Discovery
3ce20835	T1046	Network Service Discovery
7282159a	T1190	Exploit Public-Facing Application
eb949f4c	T1046	Network Service Discovery
115b8134	T1046	Network Service Discovery
7ee9ea3c	T1048	Exfiltration Over Alternative Protocol
4342f169	T1048	Exfiltration Over Alternative Protocol
e1b63d31	T1110	Brute Force / Credential Access
9fb91b42	T1110	Brute Force / Credential Access
71b53cbc	T1110	Brute Force / Credential Access
30cb8880	T1110	Brute Force / Credential Access
818bfe5f	T1110	Brute Force / Credential Access
5ebcf4b8	T1110	Brute Force / Credential Access
f7297346	T1110	Brute Force / Credential Access
0003cb34	T1048	Exfiltration Over Alternative Protocol
3cd3026c	T1046	Network Service Discovery
524cecdc	T1046	Network Service Discovery
6b699592	T1190	Exploit Public-Facing Application
8725cb13	T1110	Brute Force / Credential Access
bab5d2c9	T1110	Brute Force / Credential Access
0cb269a1	T1110	Brute Force / Credential Access
39e16d69	T1110	Brute Force / Credential Access
a2a863e8	T1110	Brute Force / Credential Access
00922d5b	T1110	Brute Force / Credential Access
e237e6d4	T1110	Brute Force / Credential Access
67856297	T1110	Brute Force / Credential Access
416414db	T1110	Brute Force / Credential Access
bab3cbf2	T1110	Brute Force / Credential Access
3f854162	T1110	Brute Force / Credential Access

Artifact ID	Technique ID	Technique Description
8ef1a913	T1110	Brute Force / Credential Access
5127eef8	T1110	Brute Force / Credential Access
c6cc4086	T1110	Brute Force / Credential Access
8706a95c	T1110	Brute Force / Credential Access
fcf354c7	T1110	Brute Force / Credential Access
c6f81156	T1110	Brute Force / Credential Access
0d3728ed	T1110	Brute Force / Credential Access
dac2f7f2	T1110	Brute Force / Credential Access
2e907ab0	T1110	Brute Force / Credential Access
d78c6b23	T1110	Brute Force / Credential Access
f12f6c63	T1046	Network Service Discovery
68f03f17	T1046	Network Service Discovery
52822cf2	T1190	Exploit Public-Facing Application
40822c6d	T1048	Exfiltration Over Alternative Protocol
aef01737	T1048	Exfiltration Over Alternative Protocol
20386212	T1048	Exfiltration Over Alternative Protocol
a82945c3	T1048	Exfiltration Over Alternative Protocol
4f0921a2	T1048	Exfiltration Over Alternative Protocol
72e2df10	T1048	Exfiltration Over Alternative Protocol
0c1d1ac7	T1005	Data from Local System
6a289230	T1005	Data from Local System
0b1b224d	T1005	Data from Local System
eb64901a	T1046	Network Service Discovery
eaf2c15f	T1046	Network Service Discovery
d4e5e5f8	T1048	Exfiltration Over Alternative Protocol
fddf3d26	T1110	Brute Force / Credential Access
04b424b8	T1110	Brute Force / Credential Access
a137c0d6	T1110	Brute Force / Credential Access
9a56bcf3	T1110	Brute Force / Credential Access
6be41566	T1110	Brute Force / Credential Access
4a837b3c	T1110	Brute Force / Credential Access
7f89897a	T1005	Data from Local System
ad350d1b	T1005	Data from Local System
1b94c894	T1005	Data from Local System
57c7bcfd	T1005	Data from Local System
5529b0cb	T1005	Data from Local System
df6bb487	T1005	Data from Local System

Artifact ID	Technique ID	Technique Description
f8baafb5	T1110	Brute Force / Credential Access
cbc89026	T1110	Brute Force / Credential Access
58cfcc58	T1110	Brute Force / Credential Access
83b2b361	T1046	Network Service Discovery
15ba0a52	T1110	Brute Force / Credential Access
1bcb272f	T1046	Network Service Discovery
bb45915f	T1190	Exploit Public-Facing Application
42ef38ce	T1110	Brute Force / Credential Access
323c6ea3	T1110	Brute Force / Credential Access
318f6fd4	T1005	Data from Local System
f2f7c9b5	T1005	Data from Local System
5e578665	T1005	Data from Local System
afe9679b	T1005	Data from Local System
ae108ba3	T1005	Data from Local System
ffc58bea	T1005	Data from Local System
a9c049e8	T1110	Brute Force / Credential Access
83a28d6c	T1110	Brute Force / Credential Access
5978f7d8	T1110	Brute Force / Credential Access
c40bb247	T1110	Brute Force / Credential Access
61b7dd8a	T1110	Brute Force / Credential Access
563d21ea	T1110	Brute Force / Credential Access
1cc91a54	T1048	Exfiltration Over Alternative Protocol
d8f97ec5	T1046	Network Service Discovery
cb892e58	T1046	Network Service Discovery
e7bce0ed	T1048	Exfiltration Over Alternative Protocol
3564d9e4	T1046	Network Service Discovery
9198e827	T1046	Network Service Discovery
f9f35444	T1190	Exploit Public-Facing Application
4ec85409	T1046	Network Service Discovery
f25bac21	T1005	Data from Local System
0e50831e	T1005	Data from Local System
47532526	T1005	Data from Local System
541a1b7e	T1005	Data from Local System
a0226f5f	T1005	Data from Local System
f71d8cc9	T1005	Data from Local System
f58add5f	T1005	Data from Local System
85446a90	T1046	Network Service Discovery

Artifact ID	Technique ID	Technique Description
de0f5eda	T1005	Data from Local System
a8bd7b9f	T1005	Data from Local System
28e6f7e7	T1005	Data from Local System
63e86720	T1005	Data from Local System
851e5019	T1005	Data from Local System
b080afa2	T1005	Data from Local System
0baea1df	T1005	Data from Local System
5d7bda47	T1046	Network Service Discovery
5a296b89	T1005	Data from Local System
112c758f	T1005	Data from Local System
e8eacd3d	T1005	Data from Local System
ccc3ee23	T1046	Network Service Discovery
d1cc772b	T1005	Data from Local System
2778adff	T1005	Data from Local System
bffff91bc	T1005	Data from Local System
a86e7d00	T1110	Brute Force / Credential Access
ab9bc982	T1046	Network Service Discovery
f740d1c7	T1046	Network Service Discovery
60a908a6	T1048	Exfiltration Over Alternative Protocol
7459e201	T1046	Network Service Discovery
6ca4bb5c	T1046	Network Service Discovery
d0ee5d82	T1046	Network Service Discovery
659c677b	T1048	Exfiltration Over Alternative Protocol
4df2b3d0	T1046	Network Service Discovery
80c353c8	T1046	Network Service Discovery
68644562	T1046	Network Service Discovery
9cc119eb	T1046	Network Service Discovery
1f03fb35	T1046	Network Service Discovery
48d3d342	T1048	Exfiltration Over Alternative Protocol
652a4177	T1048	Exfiltration Over Alternative Protocol
f6d86b2b	T1046	Network Service Discovery
80be1ff8	T1046	Network Service Discovery
d984fb19	T1046	Network Service Discovery
1d569dd8	T1046	Network Service Discovery
4f3ef6f6	T1048	Exfiltration Over Alternative Protocol
ad76efdc	T1046	Network Service Discovery
5579582b	T1048	Exfiltration Over Alternative Protocol

Artifact ID	Technique ID	Technique Description
e5375101	T1048	Exfiltration Over Alternative Protocol
24e97444	T1046	Network Service Discovery
eb4e9b98	T1046	Network Service Discovery

4. Source IP Concentration Analysis

Source IP	Event Count
74.176.56.30	72
157.20.32.130	24
93.123.109.135	24
64.62.210.38	24
82.223.9.21	6
212.52.28.106	6
103.168.21.194	6
74.234.147.76	6
128.65.195.33	6
91.204.46.136	6
20.163.78.59	6
45.56.222.60	6
160.191.139.216	6
81.88.49.27	6
66.240.223.230	6
174.142.31.70	6
194.195.245.44	6
20.184.35.52	5
129.222.187.219	4
47.52.209.228	3
194.195.86.82	3
220.158.233.50	3
80.88.86.96	3
185.187.75.18	3
197.189.255.202	3
79.137.33.241	3
3.136.197.26	3
207.38.87.177	3
15.235.203.43	3
179.108.84.136	3
104.199.79.203	3
91.107.124.38	3
222.252.11.23	3
173.199.123.6	3
51.38.109.223	3

Source IP	Event Count
41.90.64.136	3
45.227.162.235	3
34.82.67.239	3
54.37.118.70	3
87.106.120.188	2
204.76.203.212	2
43.140.247.223	2
118.70.190.36	2
95.214.55.71	1
47.128.30.224	1
47.128.30.163	1
149.50.103.48	1
47.128.19.121	1
47.128.112.137	1
176.65.148.177	1
147.185.132.234	1
129.222.147.185	1
121.127.34.151	1
222.252.11.133	1
204.76.203.18	1
154.82.150.126	1
154.82.171.11	1
156.239.204.135	1
154.82.169.248	1
156.239.206.170	1
47.128.114.191	1
34.78.138.227	1
4.190.203.84	1

5. Case Intelligence Summary

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