Digital Forensic Intelligence Report

Case ID: c15ef503

Generated: 2026-01-06 14:09:41.832236+00:00 UTC

1. Executive Summary

Incident Summary: - A large volume of external web security events were observed, dominated by ACCESS_DENIED blocks and multiple WAF_CORRELATION alerts, indicating widespread external probing. Representative evidence includes: - WAF_CORRELATION from 87.106.120.188 with accompanying SQL_INJECTION attempt: c15ef503-9bb9-4057-9b5a-3664f5af2a1a (WAF_CORRELATION) and 6f9c37f6-d047-40bc-9aad-404c23376b8a (SQL_INJECTION). - WAF_CORRELATION from 79.137.33.241 with SQL_INJECTION noted: b9931e11-8afe-4f32-86f1-e8d34335e272 (WAF_CORRELATION) and 9470dae8-b4ca-4d74-aaae-a3f86e738d99 (SQL_INJECTION); a parallel WAF_CORRELATION at 06a6163a-1cb8-4bc8-9649-c5f8ceb889d3. - WAF_CORRELATION from 3.136.197.26 with SQL_INJECTION: 62e87d40-5cdd-454a-a258-55ad88edbba2; and WAF_CORRELATION: ff26169f-1876-41de-a363-f9ad8b042632. - WAF_CORRELATION from 207.38.87.177 with SQL_INJECTION: dbbacc3b-6c9e-4ff9-bf37-ce7a4761e7af (WAF_CORRELATION) and 42488117-8f19-4f65-8eac-0defdb708a48 (SQL_INJECTION). - WAF_CORRELATION and related activity from 93.123.109.135 (938a4783...; 913a7001...; 1ed8ebf1...; 08633952...): multiple LFI indicators and WAF_CORRELATION; SQL_INJECTION observed on 93.123.109.135 as well (3b43c7ed-4a6b-4122-88fd-e91203886e60). - RCE activity from 193.142.147.209 with multiple indicators: f9b0db48-4d48-4930-8452-ce69107526b1 (RCE) and related WAF_CORRELATION: cf662829-f14d-4252-afea-66fc5689a867; additional RCE events: 3a275? series including 3ae41af0-ac67-456c-99ad-60470b0b854d, and several others. - PROTOCOL_ABUSE indicators from multiple hosts (examples): fe000091-a66b-4643-ae56-4bc38898329f (PROTOCOL_ABUSE) from 95.214.55.71; 204.76.203.212 related items (various IDs such as 5b... and 4c3ed724-8a41-4016-ab45-2d5d139cffac). - Least-privilege outcomes observed include numerous ACCESS_DENIED entries across a wide set of source IPs and target ports (examples): - 745cdd7f-5cc1-4773-9cc6-b8a3082d5feb (ACCESS_DENIED from 47.52.209.228 to port 49374) - 8f4fee9f-4938-4fa4-8a09-086d5dfccb12 (ACCESS_DENIED from 82.223.9.21 to port 38866) - bcf2b1d7-9264-4ff9-bf37-ce7a4761e7af (ACCESS_DENIED from 47.52.209.228 to port 49132) - e223d09c-3836-43b3-be35-3617c16a4ddf (ACCESS_DENIED from 82.223.9.21 to port 38832) - 49f825f0-ebd1-4d8f-ad31-0e513d683e21 (LFI indicator from 51.38.109.223 with associated ACCESS_DENIED activity) - Observed pattern indicates coordinated external probing across numerous IP addresses, with a mix of WAF_CORRELATION triggers and exploit-type indicators (SQL_INJECTION, LFI, RCE, PROTOCOL_ABUSE) and widespread access-blocks (ACCESS_DENIED). Notable artifact examples illustrate the range of observed event types and source/destination pairs: - c15ef503-9bb9-4057-9b5a-3664f5af2a1a (WAF_CORRELATION; 87.106.120.188) - 6f9c37f6-d047-40bc-9aad-404c23376b8a (SQL_INJECTION; 87.106.120.188) - 745cdd7f-5cc1-4773-9cc6-b8a3082d5feb (ACCESS_DENIED; 47.52.209.228) - 8f4fee9f-4938-4fa4-8a09-086d5dfccb12 (ACCESS_DENIED; 82.223.9.21) - fe000091-a66b-4643-ae56-4bc38898329f (PROTOCOL_ABUSE; 95.214.55.71) - b9931e11-8afe-4f32-86f1-e8d34335e272 (WAF_CORRELATION; 79.137.33.241) - 9470dae8-b4ca-4d74-aaae-a3f86e738d99 (SQL_INJECTION; 79.137.33.241) - 42488117-8f19-4f65-8eac-0defdb708a48 (SQL_INJECTION; 207.38.87.177) - dbbacc3b-6c9e-4ff9-bf37-ce7a4761e7af (WAF_CORRELATION; 207.38.87.177) - 938a4783-c500-4656-b6e2-1d7cfb35b2d4 (WAF_CORRELATION; 93.123.109.135) - f9b0db48-4d48-4930-8452-ce69107526b1 (RCE; 193.142.147.209) Notes: - No evidence in the provided artifacts of successful access or data exfiltration; multiple ACCESS_DENIED entries indicate blocking at the perimeter or application layer. - The observed activity spans numerous external IPs and ports, with varied attack vectors (SQL_INJECTION, LFI, RCE, PROTOCOL_ABUSE) and recurring WAF_CORRELATION alerts. Artifacts cited in this summary (illustrative subset): - c15ef503-9bb9-4057-9b5a-3664f5af2a1a - 6f9c37f6-d047-40bc-9aad-404c23376b8a - 745cdd7f-5cc1-4773-9cc6-b8a3082d5feb - 8f4fee9f-4938-4fa4-8a09-086d5dfccb12 - fe000091-a66b-4643-ae56-4bc38898329f - b9931e11-8afe-4f32-86f1-e8d34335e272 - 9470dae8-b4ca-4d74-aaae-a3f86e738d99 - 42488117-8f19-4f65-8eac-0defdb708a48 - dbbacc3b-6c9e-4ff9-bf37-ce7a4761e7af - 938a4783-c500-4656-b6e2-1d7cfb35b2d4 - f9b0db48-4d48-4930-8452-ce69107526b1 If you want, I can convert this into a formal incident report draft with sections for Timeline, Indicators, Impact, and Recommended Actions.

2. Case Intelligence Overview

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

Behavioral Attribute	Assessment
Attack Velocity	high
Time Pattern	business-hours
Tooling Consistency	high
Automation Likelihood	high