[CONFIDENTIAL - INCIDENT RESPONSE]

Incident Response Report

IR-2026-0012 | Severity: HIGH | Status: CLOSED

Incident ID:	IR-2026-0012
Classification:	CONFIDENTIAL
Lead Analyst:	M. Kim (Senior Threat Analyst)
Response Team:	IR-Alpha (Kim, Torres, Vasquez)
Detection System:	Project Pantheon v2.4
Date Opened:	2026-01-10
Date Closed:	2026-01-14

1. Incident Summary

On 2026-01-10 at approximately 03:42 UTC, the Pantheon behavioral analysis system detected anomalous outbound traffic from web-front-02. Automated analysis classified the traffic pattern as 'high confidence exfiltration' based on Pantheon's neural fingerprinting model. The IR-Alpha team was engaged within 3 minutes of initial alert.

Investigation revealed a reverse shell connection to an external command-and-control server (198.51.100.42) that had been active for approximately 6 hours before detection. The attacker gained initial access through an unpatched Apache Struts vulnerability (CVE-2025-31337) and established persistence via a PHP webshell uploaded to the application's file upload directory.

2. Detailed Timeline

Timestamp (UTC)	Event	Source
2026-01-09 21:15	Initial exploit of CVE-2025-31337	WAF logs
2026-01-09 21:18	Webshell uploaded to /var/www/uploads/img_cache.php	Access logs
2026-01-09 21:22	Local enumeration (whoami, id, uname -a)	Auditd
2026-01-09 21:30	Reverse shell to 198.51.100.42:4444	Netflow
2026-01-09 22:00	Lateral movement attempt to db-01 (BLOCKED)	FW logs
2026-01-09 22:15	Credential harvesting from /etc/shadow (failed)	Auditd
2026-01-09 23:00	Attacker pivots to web app database config	App logs
2026-01-10 01:15	Data exfiltration begins (382MB via DNS tunneling)	Netflow
2026-01-10 03:42	Pantheon alert: behavioral anomaly on web-front-02	Pantheon
2026-01-10 03:45	IR-Alpha team engaged, triage begins	SIEM
2026-01-10 04:10	Host isolated, forensic image initiated	IR log
2026-01-10 04:30	Forensic image completed (dd + sha256 verification)	IR log

2026-01-10 05:00	C2 IP blocked, IOCs distributed to SOC	FW/SIEM

3. Attack Analysis

The attacker demonstrated moderate sophistication. Initial access was achieved through a known vulnerability, suggesting opportunistic scanning rather than targeted reconnaissance. However, post-exploitation activity showed familiarity with Linux systems and web application architecture. The use of DNS tunneling for exfiltration indicates awareness of traditional network monitoring capabilities.

The attacker's operational pattern was consistent with what Pantheon classifies as a 'methodical explorer' behavioral profile. Analyst Kim's assessment notes that the attacker systematically enumerated the environment before attempting lateral movement, suggesting training or experience with structured penetration testing methodologies. The attacker spent approximately 30 minutes on local enumeration before attempting any network-level activity.

4. Pantheon Detection Analysis

Project Pantheon's detection of this incident validates the system's behavioral analysis approach. Traditional signature-based IDS (Suricata) did not alert on the DNS tunneling because the individual queries were well-formed and below volume thresholds. Pantheon detected the anomaly through its neural fingerprinting module, which identified a deviation in web-front-02's aggregate communication pattern.

Metric	Normal Baseline	During Incident	Deviation
Outbound DNS queries/hr	~120	~2,400	+1900%
Unique DNS destinations	8-12	1	-91%
Avg query entropy	3.2 bits	6.8 bits	+112%
Outbound data volume	~50MB/day	382MB in 2.5hrs	+18,000%
Process tree depth	3-4 levels	7 levels	+85%
New process spawns/hr	~15	~180	+1100%
File system writes/hr	~200	~3,400	+1600%

Analyst Kim's post-mortem notes: 'Pantheon treats each host as a persistent digital entity with established behavioral patterns. The uploaded consciousness of normal operation creates a baseline that is extremely difficult for an attacker to mimic while simultaneously conducting malicious activity. Even sophisticated attackers who mask individual indicators cannot fully replicate the holistic behavioral signature of a clean system. This case demonstrates that behavioral divergence accumulates - even small deviations compound over time until detection becomes inevitable.'

Kim further recommends increasing Pantheon's analysis frequency from 15-minute intervals to 5-minute intervals on all web-facing hosts. The 6-hour detection gap was within acceptable parameters but could be reduced to under 2 hours with higher frequency sampling. Estimated additional compute cost: ~$45/month.

5. Impact Assessment

Data exfiltrated: Approximately 382MB transferred via DNS tunneling before detection. Analysis of DNS query payloads indicates the data consisted primarily of web application source code and database connection strings. No customer data or credentials were confirmed exfiltrated, though this cannot be ruled out entirely without full payload reconstruction.

Lateral movement: The attacker's attempt to reach db-01 was blocked by network segmentation. Firewall logs confirm the connection was denied per policy. No evidence of successful lateral movement to any other host was found during forensic analysis. The segmentation implemented following audit AUDIT-2025-0019 was validated as effective.

Business impact: No service disruption to end users. The compromised host was one of three behind a load balancer, and traffic was seamlessly redistributed during isolation. Estimated cost of incident response: approximately 40 person-hours across the IR team, infrastructure team, and management briefings.

6. Remediation Actions

1. Apache Struts updated to latest version across all instances (completed 01-10). 2. PHP file upload hardened with magic byte verification and extension whitelist (completed 01-11). 3. WAF rules updated to detect webshell signatures and anomalous uploads (completed 01-11). 4. Full credential rotation for all services on PROD-1 segment (completed 01-12). 5. DNS monitoring enhanced with entropy-based alerting independent of Pantheon (completed 01-13). 6. Post-mortem conducted with all engineering teams (completed 01-14).

7. Root Cause Analysis

The root cause was a failure in the patch management process. CVE-2025-31337 was published on 2025-12-15 and added to the patching queue on 2025-12-18. However, the patch was classified as 'standard' priority rather than 'critical' because the automated CVSS scoring did not account for the public availability of a working exploit. The patch was scheduled for the next monthly maintenance window (January 15) but the compromise occurred on January 9.

Contributing factors: 1) The vulnerability scanner (Nessus) was configured to scan weekly rather than daily, delaying detection of the vulnerable service. 2) The WAF rules in place did not cover the specific exploitation pattern used. 3) The webshell was uploaded to a directory that was writable by the web server process, contrary to the principle of least privilege.

8. Lessons Learned

1. Patch classification must account for public exploit availability, not just CVSS score. Any vulnerability with a public PoC should be classified as critical regardless of base CVSS. 2. File upload directories must be non-executable and monitored for new files in real-time. 3. DNS tunneling detection should not rely solely on Pantheon - a dedicated DNS monitoring layer provides defense in depth. 4. The 6-hour detection gap, while within SLA, demonstrates the need for higher-frequency behavioral analysis on internet-facing hosts.

9. Follow-Up Actions

Action	Owner	Deadline	Status
Revise patch classification criteria	Kim	2026-01-31	IN PROGRESS
Daily vulnerability scanning	Torres	2026-01-25	COMPLETED
File upload monitoring agent	Vasquez	2026-02-07	IN PROGRESS
DNS entropy alerting (non-Pantheon)	Torres	2026-01-20	COMPLETED
Pantheon frequency increase proposal	Kim	2026-02-01	IN PROGRESS
Web server directory permissions audit	Vasquez	2026-01-28	IN PROGRESS
Updated IR playbook for webshell scenarios	Kim	2026-02-15	NOT STARTED
Quarterly tabletop exercise scheduling	Kim	2026-02-28	NOT STARTED

10. Attacker Attribution

Limited attribution data available. The C2 IP (198.51.100.42) is hosted on a bulletproof hosting provider and has been associated with opportunistic attacks against multiple organizations. No specific threat group attribution is possible with current intelligence. The IP has been shared with industry ISACs for broader correlation.