SECURITY INCIDENT REPORT

Incident ID:	INC-000026
Severity:	CRITICAL
Status:	OPEN
Detection Time:	2026-02-01 14:24:59 UTC
Endpoint:	EP-0048
Attack Type:	zero_day_blend

Report Generated: 2026-02-01 14:25:08

EXECUTIVE SUMMARY

A security incident was detected on endpoint **EP-0048** at 2026-02-01 14:24:59 UTC. The anomaly detection system identified suspicious behavior with an ensemble confidence of **95.0%**.

The system detected **3** MITRE ATT&CK; technique(s) associated with this incident, with the primary technique being **Brute Force**.

Current Status: **OPEN**
Severity Classification: **CRITICAL**

INCIDENT DETAILS

Model	Anomaly Score
Autoencoder	0.978
Isolation Forest	0.721
LOF	0.701
Ensemble	**0.800**
Confidence	**95.0%**

MITRE ATT&CK; TECHNIQUES

T1110: Brute Force

Tactic: Credential Access
Confidence: 95.0%
Matched Features: network_in
Description: Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained.

T1071: Application Layer Protocol

Tactic: Command and Control
Confidence: 93.5%
Matched Features: network_in, api_calls
Description: Adversaries may communicate using application layer protocols to avoid detection/network filtering.

T1190: Exploit Public-Facing Application

Tactic: Initial Access
Confidence: 61.9%

Matched Features: cpu_usage, memory_usage, network_in, api_calls
Description: Adversaries may attempt to exploit a weakness in an Internet-facing computer or program using software, data, or commands.

FEATURE ANALYSIS

Feature	Value	Baseline	Deviation	Contribution
Api Calls	614.28	100.00	6.14x	25.8%
Network In	520.73	150.00	3.47x	18.0%
Memory Usage	100.00	45.00	2.22x	11.9%
Failed Logins	1.10	0.50	2.20x	11.7%
Cpu Usage	46.84	25.00	1.87x	9.6%
Auth Attempts	3.70	2.00	1.85x	9.4%
Process Creation	5.99	5.00	1.20x	3.7%

AI EXPLANATION

Anomalous behavior detected:
• Api Calls is significantly elevated (6.1x baseline, 25.8% contribution)
• Network In is significantly elevated (3.5x baseline, 18.0% contribution)
• Memory Usage is significantly elevated (2.2x baseline, 11.9% contribution)

■■ Possible brute force attack or credential stuffing attempt

RECOMMENDED ACTIONS

1. Isolate the affected endpoint from the network immediately
2. Conduct a forensic analysis of the endpoint
3. Review and analyze related logs for the affected timeframe
4. Check for lateral movement to other systems
5. Update detection rules based on this incident
6. Implement recommended MITRE ATT&CK; mitigations