SECURITY INCIDENT REPORT

Incident ID:	INC-63644B
Severity:	CRITICAL
Status:	OPEN
Detection Time:	2026-02-04 10:14:09 UTC
Endpoint:	EP-0043
Attack Type:	crypto_mining

Report Generated: 2026-02-04 10:14:16

EXECUTIVE SUMMARY

A security incident was detected on endpoint **EP-0043** at 2026-02-04 10:14:09 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 **Exploit Public-Facing Application**.

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

INCIDENT DETAILS

Model	Anomaly Score
Autoencoder	1.000
Isolation Forest	0.772
LOF	0.837
Ensemble	**0.870**
Confidence	**95.0%**

MITRE ATT&CK; TECHNIQUES

T1190: Exploit Public-Facing Application

Tactic: Initial Access
Confidence: 67.3%
Matched Features: cpu_usage, process_creation
Description: Adversaries may attempt to exploit a weakness in an Internet-facing computer or program using software, data, or commands.

T1110: Brute Force

Tactic: Credential Access
Confidence: 46.1%
Matched Features: network_out
Description: Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained.

T1496: Resource Hijacking

Tactic: Impact
Confidence: 31.5%

Matched Features: cpu_usage, network_out, process_creation
Description: Adversaries may leverage the resources of co-opted systems to solve resource intensive problems, which may impact system availability.

FEATURE ANALYSIS

Feature	Value	Baseline	Deviation	Contribution
Cpu Usage	77.05	25.00	3.08x	16.5%
Failed Logins	0.12	0.50	0.24x	15.4%
Process Creation	11.65	5.00	2.33x	12.7%
Network Out	169.37	80.00	2.12x	11.3%
File Access	23.11	50.00	0.46x	8.2%
Api Calls	167.57	100.00	1.68x	8.2%
Auth Attempts	3.29	2.00	1.64x	7.9%

AI EXPLANATION

Anomalous behavior detected:
• Cpu Usage is significantly elevated (3.1x baseline, 16.5% contribution)
• Failed Logins is significantly reduced (0.2x baseline, 15.4% contribution)
• Process Creation is significantly elevated (2.3x baseline, 12.7% contribution)

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