SECURITY INCIDENT REPORT

Incident ID:	INC-26576D
Severity:	CRITICAL
Status:	OPEN
Detection Time:	2026-02-04 12:13:35 UTC
Endpoint:	EP-0002
Attack Type:	crypto_mining

Report Generated: 2026-02-04 12:14:00

EXECUTIVE SUMMARY

A security incident was detected on endpoint **EP-0002** at 2026-02-04 12:13:35 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	0.995
Isolation Forest	0.723
LOF	0.703
Ensemble	**0.807**
Confidence	**95.0%**

MITRE ATT&CK; TECHNIQUES

T1190: Exploit Public-Facing Application

Tactic: Initial Access
Confidence: 68.1%
Matched Features: process_creation
Description: Adversaries may attempt to exploit a weakness in an Internet-facing computer or program using software, data, or commands.

T1496: Resource Hijacking

Tactic: Impact
Confidence: 51.8%
Matched Features: process_creation
Description: Adversaries may leverage the resources of co-opted systems to solve resource intensive problems, which may impact system availability.

T1021: Remote Services

Tactic: Lateral Movement
Confidence: 51.8%

Matched Features: process_creation
Description: Adversaries may use valid accounts to log into a service specifically designed to accept remote connections.

FEATURE ANALYSIS

Feature	Value	Baseline	Deviation	Contribution
Process Creation	14.68	5.00	2.94x	20.6%
Disk Write	24.73	100.00	0.25x	19.6%
Network In	258.25	150.00	1.72x	11.1%
Dns Queries	51.39	30.00	1.71x	11.0%
Memory Usage	72.46	45.00	1.61x	10.0%
Auth Attempts	2.84	2.00	1.42x	7.8%
Disk Read	274.96	200.00	1.37x	7.2%

AI EXPLANATION

Anomalous behavior detected:
• Process Creation is significantly elevated (2.9x baseline, 20.6% contribution)
• Disk Write is significantly reduced (0.2x baseline, 19.6% contribution)
• Network In is significantly elevated (1.7x baseline, 11.1% 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