# SECURITY INCIDENT REPORT

| | |
|---|---|
| **Incident ID:** | INC-1012FA |
| **Severity:** | MEDIUM |
| **Status:** | OPEN |
| **Detection Time:** | 2026-02-01 20:05:46 UTC |
| **Endpoint:** | EP-0058 |
| **Attack Type:** | crypto_mining |

*Report Generated: 2026-02-01 20:05:45*

# EXECUTIVE SUMMARY

A security incident was detected on endpoint **EP-0058** at 2026-02-01 20:05:46 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: **MEDIUM**

# INCIDENT DETAILS

| Model | Anomaly Score |
|---|---|
| Autoencoder | 0.673 |
| Isolation Forest | 0.655 |
| LOF | 0.600 |
| | |
| **Ensemble** | **0.643** |
| **Confidence** | **95.0%** |

# MITRE ATT&CK; TECHNIQUES

### *T1190: Exploit Public-Facing Application*

**Tactic:** Initial Access
**Confidence:** 83.3%
**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.

### *T1021: Remote Services*

**Tactic:** Lateral Movement
**Confidence:** 42.0%
**Matched Features:** process_creation
**Description:** Adversaries may use valid accounts to log into a service specifically designed to accept remote connections.

### *T1496: Resource Hijacking*

**Tactic:** Impact
**Confidence:** 40.0%

**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 |
|---|---|---|---|---|
| Dns Queries | 0.00 | 30.00 | 0.00x | 30.0% |
| Cpu Usage | 82.77 | 25.00 | 3.31x | 16.0% |
| Process Creation | 13.70 | 5.00 | 2.74x | 13.6% |
| Network Out | 161.83 | 80.00 | 2.02x | 9.8% |
| Auth Attempts | 3.58 | 2.00 | 1.79x | 8.3% |
| Disk Write | 139.62 | 100.00 | 1.40x | 5.3% |
| Api Calls | 135.03 | 100.00 | 1.35x | 4.8% |

## AI EXPLANATION

Anomalous behavior detected:
• Dns Queries is significantly reduced (0.0x baseline, 30.0% contribution)
• Cpu Usage is significantly elevated (3.3x baseline, 16.0% contribution)
• Process Creation is significantly elevated (2.7x baseline, 13.6% 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