SECURITY INCIDENT REPORT

Incident ID:	INC-56FE47
Severity:	HIGH
Status:	OPEN
Detection Time:	2026-02-04 11:56:34 UTC
Endpoint:	EP-0007
Attack Type:	ransomware_deployment

Report Generated: 2026-02-04 11:56:37

EXECUTIVE SUMMARY

A security incident was detected on endpoint **EP-0007** at 2026-02-04 11:56:34 UTC. The anomaly detection system identified suspicious behavior with an ensemble confidence of **86.3%**.

The system detected **1** MITRE ATT&CK; technique(s) associated with this incident, with the primary technique being **Application Layer Protocol**.

Current Status: **OPEN**
Severity Classification: **HIGH**

INCIDENT DETAILS

Model	Anomaly Score
Autoencoder	0.959
Isolation Forest	0.653
LOF	0.538
Ensemble	**0.717**
Confidence	**86.3%**

MITRE ATT&CK; TECHNIQUES

T1071: Application Layer Protocol

Tactic: Command and Control
Confidence: 40.2%
Matched Features: api_calls
Description: Adversaries may communicate using application layer protocols to avoid detection/network filtering.

FEATURE ANALYSIS

Feature	Value	Baseline	Deviation	Contribution
Failed Logins	0.00	0.50	0.00x	25.7%
Process Creation	0.00	5.00	0.00x	25.7%
Api Calls	270.32	100.00	2.70x	11.5%
Disk Read	342.33	200.00	1.71x	6.6%

Disk Write	160.95	100.00	1.61x	6.0%
Network In	231.62	150.00	1.54x	5.6%
Dns Queries	45.43	30.00	1.51x	5.4%

AI EXPLANATION

Anomalous behavior detected:
• Failed Logins is significantly reduced (0.0x baseline, 25.7% contribution)
• Process Creation is significantly reduced (0.0x baseline, 25.7% contribution)
• Api Calls is significantly elevated (2.7x baseline, 11.5% 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