SECURITY INCIDENT REPORT

Incident ID:	INC-9291C4
Severity:	CRITICAL
Status:	OPEN
Detection Time:	2026-02-01 22:53:41 UTC
Endpoint:	EP-0029
Attack Type:	zero_day_blend

Report Generated: 2026-02-01 22:53:44

EXECUTIVE SUMMARY

A security incident was detected on endpoint **EP-0029** at 2026-02-01 22:53:41 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	0.993
Isolation Forest	0.760
LOF	0.774
Ensemble	**0.843**
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: 71.0%
Matched Features: network_in
Description: Adversaries may communicate using application layer protocols to avoid detection/network filtering.

T1190: Exploit Public-Facing Application

Tactic: Initial Access
Confidence: 49.1%

Matched Features: network_in, process_creation
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
Disk Write	0.00	100.00	0.00x	19.7%
File Access	0.00	50.00	0.00x	19.7%
Disk Read	37.37	200.00	0.19x	10.7%
Network In	498.14	150.00	3.32x	10.5%
Process Creation	13.93	5.00	2.79x	9.1%
Dns Queries	7.83	30.00	0.26x	8.7%
Memory Usage	88.67	45.00	1.97x	6.2%

AI EXPLANATION

Anomalous behavior detected:
- Disk Write is significantly reduced (0.0x baseline, 19.7% contribution)
- File Access is significantly reduced (0.0x baseline, 19.7% contribution)
- Disk Read is significantly reduced (0.2x baseline, 10.7% 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