SECURITY INCIDENT REPORT

Incident ID:	INC-EA10F8
Severity:	CRITICAL
Status:	OPEN
Detection Time:	2026-02-01 19:31:20 UTC
Endpoint:	EP-0010
Attack Type:	command_control

Report Generated: 2026-02-01 19:31:59

EXECUTIVE SUMMARY

A security incident was detected on endpoint **EP-0010** at 2026-02-01 19:31:20 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 **Exfiltration Over Alternative Protocol**.

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

INCIDENT DETAILS

Model	Anomaly Score
Autoencoder	0.999
Isolation Forest	0.618
LOF	0.812
Ensemble	**0.810**
Confidence	**95.0%**

MITRE ATT&CK; TECHNIQUES

T1048: Exfiltration Over Alternative Protocol

Tactic: Exfiltration
Confidence: 95.0%
Matched Features: dns_queries
Description: Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel.

T1110: Brute Force

Tactic: Credential Access
Confidence: 72.5%
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.

T1071: Application Layer Protocol

Tactic: Command and Control
Confidence: 50.7%

Matched Features: network_out, dns_queries, api_calls
Description: Adversaries may communicate using application layer protocols to avoid detection/network filtering.

FEATURE ANALYSIS

Feature	Value	Baseline	Deviation	Contribution
Disk Write	4.01	100.00	0.04x	25.3%
Dns Queries	144.05	30.00	4.80x	20.4%
Api Calls	298.42	100.00	2.98x	14.5%
Network Out	200.99	80.00	2.51x	12.3%
Process Creation	2.43	5.00	0.49x	6.9%
Network In	214.86	150.00	1.43x	5.5%
File Access	64.75	50.00	1.29x	4.3%

AI EXPLANATION

Anomalous behavior detected:
• Disk Write is significantly reduced (0.0x baseline, 25.3% contribution)
• Dns Queries is significantly elevated (4.8x baseline, 20.4% contribution)
• Api Calls is significantly elevated (3.0x baseline, 14.5% 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