Incident Report – BlackByte Ransomware Simulation (S1180)

Date of Simulation: August 9, 2025

Prepared by: Cybersecurity Incident Response Team - Intern

Incident ID: BB-S1180-2025

Executive Summary

A simulated ransomware incident using the BlackByte (S1180) profile was conducted to test IR readiness. The attack leveraged a JavaScript launcher (T1059.007), encrypted files using a shared key mechanism (T1486), impaired system defenses, and spread laterally across SMB shares. The response cycle included detection, containment, eradication, recovery, and post-incident review.

Attack and Detection Sequence

Time	Action	MITRE Technique
T0 – 09:40	Simulated exploit via JavaScript launcher with obfuscation	T1059.007, T1027
09:50	File encryption begins; ransom note drops in directories	T1486
09:55	Disables Defender exclusions; opens permissions with `icacls`, mounts volumes	T1562.001, T1222
10:00	Discovers SMB shares and spreads launcher	T1021.002, T1135

Detection Methods:

- **SIEM:** Monitored mass file writes and creation of ransom files (alerts triggered on write surges and specific patterns)
- **EDR + SOAR:** Detected suspicious JS execution; auto quarantined the launcher
- **Threat Intel:** Known JS loader hash matched BlackByte indicators

Response Actions:

1. Containment

a. Isolated impacted endpoints via SOAR-driven network segmentation
b. Disabled compromised user accounts; reset credentials
c. Blocked C2 domains and IPs at network perimeter

2. Eradication & Recovery

a. Removed malicious files, startup entries, and defense evasions
b. Rebuilt systems from clean golden images, applied latest patches
c. Restored data from verified backups (SHA-256 hashes confirmed)
d. Reintroduced systems in priority order, monitored closely for anomalies

3. Post-Incident Review

a. Identified root cause: lack of early detection on obfuscated JS and weak backup validation
b. Updated security policies: SIEM rules for JS loader patterns and mass-write detection
c. Shared anonymized IOCs and findings with internal CERT
d. Conducted tabletop exercise for IR team refresh

Key Takeaways

- Effective detection requires behavioral rules, not just signature-based checks for unusual JS execution or file changes.
- Rapid containment via automation (SOAR) limits ransomware spread.
- Immutable, verified backups are essential for quick recovery.
- Post-incident sharing and review improve readiness for future threats.