Threat Hunt / IR Report – LockBit Intrusion (SPARK Demo)

Prepared for: SPARK (Powered by BYO-SECAI) Demo

Date: 2026-01-27

Severity: High

Confidence: High

Executive Summary (BLUF)

An extended intrusion was identified within a Windows enterprise environment that ultimately resulted in the deployment of LockBit ransomware. The activity followed a familiar intrusion lifecycle: initial access via a trojanized installer, establishment of resilient command-and-control, credential theft, lateral movement, data exfiltration, and finally ransomware deployment.

The threat actor demonstrated strong operational discipline, maintaining multiple fallback mechanisms for persistence, access, and data theft over an eleven-day dwell period.

Initial Access

The intrusion began when a user executed a file masquerading as a legitimate Windows utility. The binary functioned as a loader that deployed a Cobalt Strike beacon, immediately establishing encrypted outbound command-and-control over HTTPS.

Observed technique highlights:

- Masquerading as a trusted Windows component

- HTTPS-based beaconing

- Use of system processes for injection

Execution & Persistence

Following execution, the threat actor rapidly deployed multiple persistence mechanisms across hosts:

- Scheduled tasks executing DLL payloads under SYSTEM context

- Registry Run key persistence for proxy tooling

- Manual and automated execution via WMI, PsExec, and batch scripts

Proxy tooling was used to maintain covert access paths even when some components were partially blocked by endpoint defenses.

Privilege Escalation & Credential Access

The actor injected into legitimate Windows processes to access LSASS memory, using high-access permission flags consistent with credential theft. Attempts were also made to extract Active Directory credentials and backup software credentials via PowerShell tooling.

Although some credential dumping attempts were blocked, sufficient credentials were obtained to enable widespread lateral movement.

Discovery & Lateral Movement

Discovery activity included:

- Active Directory enumeration

- Domain controller identification

- Process and software inventory collection

Lateral movement was conducted using:

- SMB and remote service creation

- RDP for interactive access

- WinRM and WMI for remote command execution

File servers and backup servers were prioritized as pivot points and staging systems.

Command and Control

Command-and-control was maintained through:

- Cobalt Strike HTTPS beacons

- SystemBC proxy infrastructure

- GhostSOCKS malware-as-a-service proxy tooling

Multiple C2 domains and IPs were used, providing redundancy and resilience over the intrusion lifecycle.

Data Exfiltration

Data exfiltration occurred in multiple phases:

1. Initial testing using anonymous file-sharing services

2. Large-scale exfiltration using Rclone over cloud storage (MEGA)

3. Follow-on exfiltration via FTP to attacker-controlled servers

Exfiltration persisted for extended periods, indicating limited detection or enforcement controls.

Impact

On the eleventh day, the threat actor executed a coordinated ransomware deployment:

- Centralized staging via a shared directory

- Distribution using PsExec, WMI, and BITSAdmin

- Execution of LockBit ransomware across accessible Windows hosts

The deployment was automated with multiple fallback scripts to ensure completion despite partial failures.

Time to Ransomware: ~11 days (239 hours)

Key Indicators (Validated)

Network Indicators

- accessservicesonline[.]com

- compdatasystems[.]com

- user.compdatasystems[.]com

- retailadvertisingservices[.]com

- 31.172.83.162:443

- 159.100.14.254:443

- 185.236.232.20:445

- 38.180.61.247:30001

- 195.2.70.38:30001

- 91.142.74.28:30001

- 93.115.26.127:21

- 46.21.250.52:21

File Hashes (SHA-256)

- setup_wm.exe: d8b2d883d3b376833fa8e2093e82d0a118ba13b01a2054f8447f57d9fec67030

- svcmc.dll: ced4ee8a9814c243f0c157cda900def172b95bb4bc8535e480fe432ab84b9175

- svcmcc.dll: 44cf04192384e920215f0e335561076050129ad7a43b58b1319fa1f950f6a7b6

- svchosts.exe: b4ad5df385ee964fe9a800f2cdaa03626c8e8811ddb171f8e821876373335e63

- check.exe: 3f97e112f0c5ddf0255ef461746a223208dc0846bde2a6dca9c825d9c706a4e9

- ds.exe (LockBit): 59c9d10f06f8cb2049df39fb4870a81999fd3f8a79717df9b309fadeb5f26ef9

MITRE ATT&CK; Coverage (Selected)

- T1036.005 – Masquerading

- T1055 – Process Injection

- T1003.001 – LSASS Credential Dumping

- T1053.005 – Scheduled Task Persistence

- T1090 – Proxy

- T1021.002 – SMB Lateral Movement

- T1021.001 – RDP

- T1048 – Exfiltration Over Alternative Protocol

- T1486 – Data Encrypted for Impact

Analyst Notes (SPARK Context)

This report demonstrates a full end-to-end intrusion lifecycle suitable for SPARK demo purposes:

- Realistic dwell time

- Multiple overlapping techniques

- Clear transitions from access → theft → extortion

The indicators and behaviors presented here are appropriate for generating:

- Threat Hunt Packages

- Findings

- Detection Strategy (ADS) artifacts

- Executive-level summaries