SECURITY INCIDENT NARRATIVE

INCIDENT DETAILS

Incident Type:

Ransomware Attack - Data Encryption and Exfiltration

Date/Time Detected:

December 18, 2025 at 03:47 UTC (23:47 EST December 17, 2025)

Affected Systems:

Production file servers (FS-PROD-01, FS-PROD-02, FS-PROD-03), Finance department workstations (12 endpoints), Customer database backup server (DB-BACKUP-01), VPN gateway (VPN-GW-02)

Threat Actor Assessment:

Based on ransom note language patterns, encryption methodology (AES-256 with RSA-4096), and TTP analysis, the incident exhibits characteristics consistent with the LockBit 3.0 ransomware operation. Attack infrastructure traced to Tor hidden services previously associated with this threat group. Likely financially motivated cybercriminal organization with previous history targeting mid-size financial services firms.

Initial Attack Vector:

Spear-phishing email sent to finance@company.com on December 15, 2025 containing malicious macro-enabled Excel document disguised as vendor invoice. Document title: "Invoice_Q4_2025_URGENT.xlsm". User in Finance department enabled macros, executing initial payload. Secondary persistence established via scheduled task and registry modification. Lateral movement detected 36 hours post-initial compromise using compromised domain admin credentials harvested via credential dumping (LSASS memory).

Data/Assets at Risk:

• Customer Personally Identifiable Information (PII): Approximately 47,500 customer records containing names, addresses, phone numbers, email addresses, and account numbers
• Financial Records: Q3-Q4 2025 transaction data, general ledger entries, accounts payable/receivable databases
• Employee Data: HR records for 156 employees including SSNs, salary information, performance reviews, healthcare enrollment data
• Intellectual Property: Product development roadmaps, proprietary pricing algorithms, competitive analysis documents
• Backup Systems: Encrypted backup repositories potentially compromised, affecting disaster recovery capabilities
• Business Operations: Critical business systems offline, affecting customer service, payment processing, and reporting functions

SUPPORTING DOCUMENTATION

Evidence Summary:

Network traffic captures from firewall and IDS systems show suspicious outbound connections to IP addresses 185.220.101.42 and 192.42.116.180 (both Tor exit nodes) beginning December 17, 2025 at 22:15 UTC. Approximately 14.7 GB of data exfiltrated over encrypted channel prior to encryption event.

Endpoint Detection and Response (EDR) logs captured malicious PowerShell execution, including use of Invoke-Mimikatz for credential harvesting and PSExec for lateral movement. Process hollowing technique detected in svchost.exe instances.

Disk forensics of patient zero workstation (FIN-WKS-07) recovered deleted temporary files including dropper payload (SHA256: 8f4e33f3dc3e414ff94e5fb6905cba8c98b4334a), staging scripts, and enumeration tools.

Ransom note deposited in multiple directories contains unique victim ID, Tor-based payment portal URL, and demand for 45 Bitcoin (approximately $1.89 million USD at current exchange rates) with 72-hour deadline before threatened public data disclosure.

Email server logs confirm phishing email delivery to finance@company.com distribution list on December 15, 2025 at 14:23 UTC. Email header analysis reveals spoofed sender address mimicking legitimate vendor domain with minor typosquatting variation.

Security Information and Event Management (SIEM) correlation identified failed login attempts across multiple administrative accounts in the 6-hour period preceding the encryption event, suggesting reconnaissance and privilege escalation activities.

CURRENT CONTAINMENT STATUS

Actions Completed:

- All affected systems isolated from production network at 04:15 UTC December 18
- Internet egress blocked for finance department VLAN
- VPN gateway taken offline and all active VPN sessions terminated
- Domain admin credentials rotated; all privileged accounts forced password reset
- Forensic images captured of three critical servers and patient zero workstation
- Incident response team assembled and war room established
- Threat intelligence shared with FBI Cyber Division and IC3
- External cybersecurity incident response firm (Mandiant) engaged at 06:30 UTC
- Legal counsel and cyber insurance carrier notified
- Preliminary employee communication sent to staff regarding system outages

Actions In Progress:

- Comprehensive network-wide malware scan using updated signatures (65% complete)
- Memory forensics analysis of additional potentially compromised endpoints
- Complete Active Directory security audit and account review
- Restoration of critical systems from verified clean backup snapshots (offline backups from December 10, 2025 confirmed unencrypted)
- Assessment of data exfiltration scope through network flow analysis
- Coordination with law enforcement on threat actor attribution and potential recovery options
- Development of customer notification communications pending legal review
- Evaluation of decryption options (ransom payment decision pending executive approval)

Containment Effectiveness:

Based on current indicators, adversary access has been successfully terminated. No new malicious activity detected since isolation measures implemented. Monitoring continues for persistence mechanisms or secondary command and control channels. Affected systems remain isolated pending complete remediation and validation. Business operations partially restored using manual processes and offline backup systems.

--- END OF INCIDENT NARRATIVE ---