DIGITAL FORENSIC LOG EVIDENCE

Case Reference: INC-2025-001847

Evidence Collection Date: December 18-22, 2025

INCIDENT CLASSIFICATION

Incident Type: Ransomware Attack with Data Exfiltration

Attack Vector: Phishing email with malicious attachment

Malware Family: LockBit 3.0 variant

Severity Level: CRITICAL

AFFECTED SYSTEMS AND INFRASTRUCTURE

System ID	Hostname	IP Address	OS	Status
SRV-001	DC-PRIMARY.corp.local	10.50.10.5	Windows Server 2019	Compromised
SRV-012	FILE-SRV-01.corp.local	10.50.10.18	Windows Server 2022	Encrypted
SRV-019	SQL-PROD-01.corp.local	10.50.10.25	Windows Server 2019	Encrypted
WKS-147	ACCOUNTING-PC12	10.50.20.147	Windows 11 Pro	Patient Zero
WKS-203	HR-LAPTOP-08	10.50.20.203	Windows 10 Pro	Compromised
NET-FW-01	FIREWALL-PERIMETER	203.0.113.45	Cisco ASA 5525-X	Affected

EVIDENCE COLLECTION INVENTORY

Evidence Item EV-001: Full disk image of WKS-147 (Patient Zero)

- Storage: 512GB NVMe SSD (Samsung 980 PRO)
- Hash (SHA-256): a3f5d8c2e1b6f9a4d7c8e2b5f1a6d9c3e7b4f8a2d6c9e3b7f1a5d8c2e6b9f4a7
- Collection Method: FTK Imager 4.7.1
- Collection Date/Time: 2025-12-18 14:23:17 UTC

Evidence Item EV-002: Memory dumps from compromised servers

- SRV-001 RAM dump (32GB) - Hash: b7e4f1a9d2c5e8b3f6a9d1c4e7b2f5a8d3c6e9b4f7a2d5c8e1b6f9a4d7c3e8b5
- SRV-012 RAM dump (64GB) - Hash: c8f5a2b6d9e3c7f1a4b8d2e6c9f3a7b5d1e8c4f9a6b3d7e2c5f8a1b6d9e4c7f2
- Collection Tool: Magnet RAM Capture 1.2.0

Evidence Item EV-003: Network traffic captures (PCAP files)

- Time Range: 2025-12-17 09:00:00 to 2025-12-18 18:00:00 UTC
- Total Capture Size: 47.3 GB
- Capture Points: Perimeter firewall, internal switches (VLANs 10, 20, 30)
- Hash: d9e6c3f8a5b2d7e4c1f9a6b3d8e5c2f7a4b9d6e3c8f1a5b2d7e4c9f6a3b8d5e2

Evidence Item EV-004: System and security logs

- Windows Event Logs (Security, System, Application) - All affected hosts
- Firewall logs (Cisco ASA syslog) - 2.1M entries
- EDR telemetry (CrowdStrike Falcon) - 850K events
- Email gateway logs (Proofpoint) - 145K messages

Evidence Item EV-005: Malware samples and artifacts

- Initial dropper: invoice_dec2024.doc.exe (2.4 MB)
  Hash: e7f2a5b8d1c6e9f4a3b7d2e5c8f1a6b9d4e7c2f8a5b3d6e9c4f7a2b5d8e1c6f9
- Ransomware binary: svchost.exe (4.8 MB) - Masquerading as legitimate process
  Hash: f8a3b6d9e2c7f4a1b5d8e3c6f9a4b7d2e5c8f1a6b9d4e7c3f8a2b5d6e9c4f7a3
- Ransom note: README_TO_DECRYPT.txt

CHRONOLOGICAL TIMELINE OF EVENTS

Date/Time (UTC)	Event Description	Source
2025-12-17 09:14:23	Phishing email received by user jsmith@corp.local with subject 'Urgent: December Invoice Payment'	Email Gateway Logs
2025-12-17 09:18:45	User jsmith opened malicious attachment invoice_dec2024.doc.exe	EDR Telemetry
2025-12-17 09:18:52	Initial payload executed, created scheduled task 'WindowsUpdateCheck'	WKS-147 Event Log
2025-12-17 09:19:15	Outbound connection to C2 server 185.220.101.47:443 established	Firewall Logs
2025-12-17 09:24:38	Lateral movement attempt via SMB to SRV-001 using compromised credentials	Network Traffic
2025-12-17 11:47:22	Active Directory enumeration detected (LDAP queries)	DC Event Logs
2025-12-17 14:33:09	Credential dumping activity detected (LSASS access)	EDR Alert
2025-12-17 18:22:45	Data exfiltration to 203.0.113.89:8443 (5.7 GB transferred)	Firewall Logs
2025-12-18 02:15:33	Ransomware deployment initiated across network	Multiple Sources
2025-12-18 02:16:01	File encryption begins on FILE-SRV-01	File System Logs
2025-12-18 02:18:47	SQL database encryption on SQL-PROD-01	SQL Server Logs
2025-12-18 06:32:15	First user report of inaccessible files to IT helpdesk	Ticket System
2025-12-18 06:45:00	Incident response team activated	IR Documentation
2025-12-18 07:00:00	Network isolation procedures initiated	IR Documentation
2025-12-18 14:00:00	Forensic evidence collection begins	Chain of Custody

FORENSIC TOOLS AND METHODOLOGIES

Tool Category	Tool Name	Version	Purpose
Disk Imaging	FTK Imager	4.7.1	Forensic disk acquisition
Memory Analysis	Volatility	3.2.0	RAM dump analysis and artifact extraction
Network Analysis	Wireshark	4.0.11	PCAP file analysis and protocol dissection
Malware Analysis	IDA Pro	8.3	Reverse engineering of malicious binaries
Log Analysis	Splunk Enterprise	9.1.2	Centralized log aggregation and analysis
Timeline Analysis	Plaso/log2timeline	20231130	Super timeline generation
File Analysis	Autopsy	4.21.0	File system and artifact analysis
Registry Analysis	RegRipper	3.0	Windows Registry parsing
OSINT	VirusTotal API	v3	Malware hash reputation checks
Reporting	AXIOM	7.8	Evidence management and reporting

PRELIMINARY FINDINGS AND INDICATORS OF COMPROMISE

Initial Access Vector:

- Spear-phishing email bypassed email security filters
- Social engineering tactics leveraged legitimate-appearing invoice theme
- User jsmith@corp.local clicked malicious attachment at 09:18:45 UTC

Command and Control Infrastructure:

- Primary C2: 185.220.101.47:443 (Tor exit node, Netherlands)
- Secondary C2: 203.0.113.89:8443 (VPS, offshore hosting)
- Communication protocol: HTTPS with custom SSL pinning
- Beacon interval: 300 seconds (5 minutes)

Persistence Mechanisms:

- Scheduled Task: \Microsoft\Windows\WindowsUpdate\WindowsUpdateCheck
Command: C:\Windows\Temp\svchost.exe -silent
- Registry Run Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\SecurityUpdate
- Service Creation: 'Windows Security Update Service' (malicious)

Credential Compromise:

- 47 domain accounts compromised via LSASS memory dumping
- Domain Admin credentials obtained: corp\administrator
- Kerberos Golden Ticket artifacts identified in memory
- Pass-the-Hash attacks observed across multiple systems

Data Exfiltration:

- Total data exfiltrated: 5.7 GB over 6-hour period
- Targeted directories:
- \\FILE-SRV-01\Finance\Confidential
- \\FILE-SRV-01\HR\Personnel_Records
- \\SQL-PROD-01\Backups\Customer_Database
- Exfiltration method: HTTPS POST requests to 203.0.113.89:8443/upload
- Compression: RAR archives with password protection

Ransomware Deployment:

- Encryption algorithm: AES-256 with RSA-4096 key exchange
- File extensions targeted: .docx, .xlsx, .pdf, .pst, .sql, .mdb, .jpg, .png, +120 others
- Total files encrypted: 1,247,839 files across network
- Encrypted file extension: .lockbit3
- Ransom demand: 50 Bitcoin (~$2.1M USD at time of incident)
- Payment wallet: bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Lateral Movement Techniques:

- SMB exploitation via EternalBlue variant (CVE-2017-0144)
- PsExec deployment for remote code execution
- WMI (Windows Management Instrumentation) for remote process creation
- RDP sessions with compromised credentials

Malware Analysis Summary:

- Malware Family: LockBit 3.0 (Black variant)
- First seen in wild: October 2024
- VirusTotal detection: 58/72 engines (80.6%)

- Anti-analysis techniques: VM detection, debugger detection, code obfuscation
- Communication encryption: Custom XOR + AES hybrid

Key File Hashes (IOCs):

File Name	SHA-256 Hash	Description
invoice_dec2024.doc.exe	e7f2a5b8d1c6e9f4a3b7d2e5c8f1a6b9d4e7c2f8a5...	Initial dropper payload
svchost.exe	f8a3b6d9e2c7f4a1b5d8e3c6f9a4b7d2e5c8f1a6b9...	Ransomware binary (main)
explorer.dll	a9d4e7c2f8b5d1e6c3f9a4b7d2e5c8f1a6b9d4e7...	Persistence module
update.bat	b2e5c8f1a6b9d4e7c3f8a2b5d6e9c4f7a1b8d3e6...	Cleanup script

Network Indicators (IOCs):

IP Address	Port	Type	Geolocation
185.220.101.47	443	C2 Server (Primary)	Amsterdam, NL
203.0.113.89	8443	Exfiltration Server	Offshore
198.51.100.156	80	Secondary C2	Unknown
192.0.2.45	443	Update Server	Germany
