Security Operations Center

Incident Analysis & Threat Intelligence Journal

Analyst: Lydiah Muigwa | Classification: Internal Use | Review Period: Q3 2025

Incident Analysis #001 | CRITICAL | Ransomware Campaign

Date: July 23, 2025 | Classification: Healthcare Sector Breach

EXECUTIVE SUMMARY

Incident Type: Ransomware deployment via spear-phishing vector
Sector: Healthcare (HIPAA-regulated entity)
NIST Phase: Detection & Analysis → Containment & Recovery
Business Impact: Complete operational shutdown requiring external incident response assistance

TECHNICAL ANALYSIS & TOOLS

Primary Analysis: Manual incident reconstruction from organizational response documentation
Framework Applied: NIST SP 800-61r2 Computer Security Incident Handling Guide
Methodology: Post-incident forensic timeline reconstruction and root cause analysis

THREAT INTELLIGENCE ASSESSMENT (5W ANALYSIS)

Threat Actor (WHO): Organized cybercriminal group with healthcare sector targeting pattern. Exhibited sophisticated operational security and encryption capabilities consistent with established ransomware-as-a-service operations.

Attack Vector (WHAT): Multi-stage ransomware deployment:
- Initial compromise via spear-phishing email
- Lateral movement through domain credentials
- Data exfiltration prior to encryption
- Double-extortion technique (encryption + data theft)

Timeline (WHEN): Tuesday, 09:00 PST - Initial detection of encrypted systems
- Estimated dwell time: 72-96 hours based on encryption scope
- Peak encryption activity: 06:00-09:00 PST (off-hours deployment)

Target Environment (WHERE): Healthcare organization infrastructure
- Electronic Health Records (EHR) systems
- Patient database servers
- Administrative workstations
- Backup systems (indicating reconnaissance phase)

Motivation Analysis (WHY): Financial extortion with compliance leverage
- Healthcare data commands premium ransom pricing

- HIPAA compliance pressures accelerate payment decisions
- Critical infrastructure disruption maximizes pressure
- Double-extortion increases success probability

BUSINESS IMPACT ASSESSMENT

Operational Impact: Complete service disruption requiring emergency protocols
Regulatory Implications: Potential HIPAA breach notification requirements
Recovery Strategy: External IR firm engagement + federal law enforcement coordination
Lessons Learned: Critical gaps in backup isolation and email security controls

STRATEGIC RECOMMENDATIONS

Immediate Actions:

- Implement email security gateway with advanced threat protection
- Deploy endpoint detection and response (EDR) across all systems
- Establish air-gapped backup strategy with 3-2-1 methodology

Long-term Initiatives:

- Zero-trust network architecture implementation
- Quarterly red team exercises focused on healthcare attack vectors
- Security awareness training with phishing simulation program

Threat Intel Investigation #002 | HIGH | Malware Analysis

Date: July 27, 2025 | Classification: Advanced Persistent Threat Indicators

EXECUTIVE SUMMARY

Investigation Type: Suspicious file hash analysis and threat attribution
Target Sector: Financial Services
NIST Phase: Detection & Analysis
Threat Classification: Confirmed malicious executable with multi-stage payload delivery

TECHNICAL ANALYSIS & INTELLIGENCE TOOLS

Primary Platform: VirusTotal Enterprise API integration
Analysis Depth: Static analysis, behavioral indicators, threat intelligence correlation
Attribution Sources: Commercial threat intel feeds, OSINT collection, industry CTI sharing
MITRE ATT&CK Mapping: T1566.001 T1204.002 T1059.001

THREAT INTELLIGENCE ASSESSMENT (5W ANALYSIS)

Threat Actor (WHO): APT group with financial services targeting pattern. Techniques consistent with FIN7/Carbanak operations based on TTPs and infrastructure overlap from threat intelligence correlation.

Attack Methodology (WHAT): Sophisticated spear-phishing campaign:
- Social engineering targeting finance personnel
- Password-protected malicious attachment bypass
- Multi-stage malware deployment with living-off-the-land techniques
- Credential harvesting and lateral movement preparation

Attack Timeline (WHEN):
- 13:11 PST - Initial phishing email delivery
- 13:13 PST - Attachment download and execution
- 13:15 PST - Secondary payload deployment
- 13:20 PST - IDS signature triggered and alert generated

Target Environment (WHERE): Financial services organization workstation
- Employee system with access to customer data repositories
- Network segment: Corporate LAN with domain connectivity
- Potential for lateral movement to core banking systems

Threat Motivation (WHY): Financial data theft and persistent access establishment
- High-value target: financial customer data and transaction systems
- Social engineering exploits employee trust and authority
- Sophisticated evasion techniques indicate advanced threat capability

MALWARE ANALYSIS DETAILS

File Hash (SHA-256):

```
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
```

VirusTotal Detection: 45/70 security vendors flagged as malicious
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
Behavioral Indicators: Registry modification, network callbacks, process injection
C2 Infrastructure: Multiple domains with fast-flux DNS patterns

RISK ASSESSMENT & BUSINESS IMPACT

Immediate Risk: Compromised workstation with potential for data exfiltration
Compliance Risk: PCI-DSS, SOX, and state privacy law implications
Operational Impact: Contained to single endpoint with rapid response
Reputation Risk: Minimal due to effective detection and containment

TACTICAL & STRATEGIC RECOMMENDATIONS

Immediate Containment:

- Network isolation of affected workstation
- Password reset for affected user account
- IOC hunting across enterprise infrastructure

Process Improvements:

- Enhanced email security controls with attachment sandboxing
- User behavior analytics for anomalous authentication patterns
- Quarterly security awareness training with simulated phishing campaigns

Intelligence Integration:

- Subscribe to financial sector threat intelligence feeds
- Implement automated IOC ingestion from industry sharing groups
- Establish threat hunting program focused on financial sector TTPs

Document Control:
Classification: Internal Use Only | Version: 1.0 | Next Review: October 2025
Distribution: SOC Team, Threat Intelligence, Management