COMPREHENSIVE DIGITAL FORENSICS INVESTIGATION REPORT

THE PHANTOM BREACH: BANKING TROJAN ATTACK

CASE ID: NXT-2025-DFIR-042
ORGANIZATION: NexusTech Financial Services
INVESTIGATION TEAM: Omar Ebeid
DATE OF REPORT: April 12, 2025
CLASSIFICATION: CRITICAL — Confirmed Data Breach & Financial Fraud

CONFIDENTIAL
Distribution of this report is restricted to authorized personnel only

DOCUMENT INFORMATION

Document Title	Comprehensive Digital Forensics Investigation Report: The Phantom Breach
Document ID	NXT-2025-DFIR-042-R1
Version	1.0
Status	Final
Date	April 12, 2025
Author(s)	Digital Forensics Team
Reviewer(s)	Chief Information Security Officer, Head of Legal Department
Classification	CONFIDENTIAL

REVISION HISTORY

Version	Date	Author	Description
0.1	April 8, 2025	DFIR Team	Initial draft
0.2	April 10, 2025	DFIR Team	Added network forensics findings
1.0	April 12, 2025	DFIR Team	Final version

Contents

EXECUTIVE SUMMARY

On April 4, 2025, NexusTech Financial Services detected suspicious outbound network traffic at 2:13 AM EST from their main transaction processing server (PROD-TX01). The anomalous activity triggered automated security alerts, prompting immediate investigation. Initial assessment indicated unauthorized financial transactions totaling several million dollars had been redirected to unknown accounts, along with potential exfiltration of sensitive customer data.

This comprehensive report details the findings of the forensic investigation across multiple evidence sources: disk images, memory dumps, network traffic, and system logs. The investigation confirms that NexusTech was the victim of a sophisticated multi-stage attack involving a PDF-based phishing email, banking trojan deployment, and data exfiltration. The attack bears the hallmarks of two sophisticated financially-motivated threat actors working in tandem or succession: initial compromise via techniques consistent with FIN7, followed by ransomware deployment attempts associated with both DarkSide and LockBit.

The investigation successfully reconstructed the complete attack chain, identified the primary attack vector, documented lateral movement, and established a comprehensive timeline of events. Countermeasures have been implemented to contain the breach, and this report provides strategic recommendations for strengthening security posture against similar threats in the future.

ALERT

Key findings indicate a sophisticated attack chain: phishing email → malicious PDF → banking trojan → data exfiltration → ransomware preparation.

Chapter 1

INVESTIGATION OVERVIEW

1.1 Scope & Objectives

The investigation focused on:

1. Identifying the initial attack vector and entry point
2. Determining the full scope and timeline of the compromise
3. Identifying impacted systems and data
4. Documenting tactics, techniques, and procedures (TTPs)
5. Collecting indicators of compromise (IOCs)
6. Providing actionable remediation recommendations

1.2 Key Questions Addressed

1. How did the attackers gain initial access?
2. What systems were compromised?
3. What data was accessed or exfiltrated?
4. What actions did the attackers take on the network?
5. How long did the attackers have access?
6. How was the attack detected?
7. What threat actor(s) were responsible?

1.3 Investigation Team

- Digital Forensics Analysts
- Network Security Specialists
- Malware Analysts
- Incident Response Team

Chapter 2

EVIDENCE COLLECTION & HANDLING

2.1 Evidence Sources

Evidence Type	Description	Collection Date	Hash (SHA256)
Disk Image	PROD-TX01 Server	April 4, 2025	casestudy.001: [REDACTED]
Memory Dump	PROD-TX01 Server	April 4, 2025	memdump.raw: [REDACTED]
PCAP	Network Traffic	April 4, 2025	networkForensics.pcapng: [REDACTED]
System Logs	Windows Event Logs	April 4, 2025	EVTX files: [REDACTED]
Email	Outlook MSG file	April 4, 2025	[REDACTED]

Table 2.1: Digital Evidence Collected

2.2 Chain of Custody

All evidence was collected following best practices in digital forensics to maintain integrity and admissibility. Write-blockers were used during acquisition, and forensic images were verified using cryptographic hashes. All actions were documented in the chain of custody log (see Appendix A).

2.3 Analysis Environment

The investigation was conducted in an isolated forensic laboratory using industry-standard tools:

- FTK Imager for disk acquisition

- Volatility 3 for memory analysis
- Wireshark/Tshark for network analysis
- Autopsy for disk forensics
- Custom forensic scripts and plugins

Chapter 3

TECHNICAL ANALYSIS

3.1 Email Analysis

3.1.1 Metadata Analysis

The attack began with a targeted phishing email sent to an employee (johntravolt2025@outlook.com) on April 4, 2025:

Field	Value	Analysis
From	Ryan Smith <mandtorycheck2025@outlook.com>	Suspicious sender, note misspelling of "mandatory"
To	johntravolt2025@outlook.com	Target employee
Subject	Urgent: Banking Security Update Required	Classic urgency trigger
Date	Fri, 4 Apr 2025 17:04:32 +0000	Outside business hours
Attachment	Security_Update_2025.pdf	Malicious payload

Table 3.1: Email Metadata Analysis

The email passed all standard email authentication checks (SPF, DKIM, DMARC), suggesting the attackers either:

- Compromised a legitimate Outlook account
- Created a new account that passed Microsoft's security checks
- Used a specially crafted domain with proper email authentication

3.1.2 Email Content Analysis

The email used a sophisticated social engineering approach:

- Impersonated a security team with authentic-looking branding
- Created urgency through warnings about "cyber threats"

- Demanded action by claiming the update was "MANDATORY"
- Set a deadline (March 20, 2025) to create time pressure
- Contained professional formatting with security-themed language

3.2 Malicious PDF Analysis

3.2.1 Static Analysis

The malicious PDF (Security_Update_2025.pdf) contained embedded JavaScript designed to trigger upon opening:

Attribute	Value
File Name	Security_Update_2025.pdf
Size	3.42 KB
SHA256	dbfc7d718c7899ef17bf50ff921b4855dfa9d0ac9599564af43488ed1e4dbe69
Creation Date	April 4, 2025 13:19 UTC
Detection	Flagged by DOCGuard (1/63 on VirusTotal)

Table 3.2: PDF Malware Attributes

Analysis with PDF examination tools (pdfid.py and pdf-parser.py) revealed:

- `/JavaScript` objects present
- `/OpenAction` and `/AA` (auto actions) configured
- Suspicious embedded JavaScript code

3.2.2 Dynamic Analysis

Sandbox analysis of the PDF revealed:

- Execution of embedded JavaScript code
- Attempted connection to IP 192.168.20.200 over HTTP
- Attempted download of a batch file: `deploy_pdf_payload.bat`
- Creation of files in Adobe Reader temporary directories

3.2.3 MITRE ATT&CK Mapping

The PDF utilized these techniques:

- **TA0002**: Execution
- **T1059.007**: JavaScript execution
- **T1566.001**: Spearphishing Attachment
- **T1204.002**: User Execution: Malicious File

3.3 Memory Forensics

Memory analysis of PROD-TX01 using Volatility 3 revealed several suspicious processes and activities:

3.3.1 Process Analysis

PID	Parent PID	Process Name	Creation Time	Termination Time	Suspicion
6848	9308	powershell.exe	2025-04-05 02:49:10	2025-04-05 02:49:44	Zero threads, zero handles, unknown parent
7260	6848	msiexec.exe	2025-04-05 02:49:44	N/A	Spawned by suspicious PowerShell process
2960	3684	xampp-control.exe	2025-04-04 16:02:10	N/A	Unexpected web server on financial system
1292/7689	2960	httpd.exe	2025-04-04 16:02:15/17	N/A	Apache server for C2 communications
7788	2960	mysqld.exe	2025-04-04 16:02:19	N/A	Database for data staging

Table 3.3: Suspicious Processes Identified in Memory

3.3.2 Memory Injection Detection

Analysis of the `msiexec.exe` process (PID 7260) using the `malfind` plugin identified highly suspicious memory regions:

Start Address	Protection	Content	Analysis
0x4550000	PAGE_EXECUTE_READWRITE	0x0: add byte ptr [eax], al	RWX memory - typical for shellcode/process injection

Table 3.4: Memory Injection Evidence

Custom memory scanning revealed the presence of signatures matching both DarkSide and LockBit ransomware, indicating the attackers were preparing for a ransomware attack after data exfiltration.

3.3.3 Network Connections in Memory

Memory forensics identified active network connections from compromised processes to suspected command and control servers, including connections from `httpd.exe` and `powershell.exe` to external addresses.

3.4 Disk Forensics

Analysis of the disk image from PROD-TX01 revealed:

3.4.1 Timeline Analysis

Timestamp	Activity	Location	Notes
2025-04-04 13:19	Security_Update_2025.pdf created	Desktop	Initial infection vector
2025-04-04 16:02:10	XAMPP installed	C:\xampp	Web server for C2
2025-04-04 16:02:15	Apache HTTP server started	C:\xampp\apache	Command & control server
2025-04-04 16:02:19	MySQL server started	C:\xampp\mysql	Database for staging data
2025-04-05 02:49:10	PowerShell executed	%TEMP%	Suspicious execution
2025-04-05 02:49:44	MSI package executed	%TEMP%	Malware installation

Table 3.5: Key Events from Disk Timeline

3.4.2 Filesystem Analysis

- Modified PHP files in C:\xampp\htdocs showing web-based backdoor code
- Evidence of a banking trojan implemented as a PHP backdoor that:
  - Intercepted login credentials
  - Captured transaction data
  - Modified transaction amounts (skimming 10%)
  - Stole database credentials
- Scheduled task creation for persistence

- Evidence of batch files and PowerShell scripts designed to:
  - Download additional payloads
  - Establish persistence
  - Disable security controls

3.5 Network Forensics

Analysis of the network traffic capture (networkForensics.pcapng) revealed multiple suspicious activities:

3.5.1 Protocol Analysis

Protocol	Count	Suspicious Activity
UDP	395 frames	LLMNR/NBNS spoofing attempts
SMB over NetBIOS	12 frames	Potential lateral movement
HTTP	Multiple	C2 communications, data exfiltration

Table 3.6: Network Protocol Analysis

3.5.2 Attacker Infrastructure

IP Address	Role	Activity
192.168.20.10	Attacker	Source of LLMNR/NBNS queries, credential harvesting attempts
192.168.20.1	Victim	Repeatedly attempted to resolve "Admin"
192.168.20.200	C2 Server	Hosted malicious payloads and received exfiltrated data

Table 3.7: Network Infrastructure Identified

3.5.3 Attack Techniques

The network traffic showed clear evidence of:

- Attempted LLMNR/NBNS name poisoning (likely using Responder)
- Reconnaissance scanning of internal systems
- Command and control traffic to attacker infrastructure
- Data exfiltration via HTTP POST requests
- Attempts to relay credentials to gain further access

3.6 Log Analysis

Windows Event Logs provided critical insights into the attack progression:

3.6.1 Suspicious System Events

Event ID	Description	Timestamp	Significance
7040	BITS service repeatedly modified	4/6/2025 4:07 AM - 5:54 AM	Abused for persistent data transfers
41	Unexpected system reboot	4/6/2025 4:01:44 AM	Possible crash from exploitation
1796	Secure Boot not enabled	4/6/2025 4:06:48 AM	System vulnerable to boot-level malware
50, 140	Critical volume write failures	4/5/2025 10:52 AM	Potential data corruption/anti-forensics

Table 3.8: Suspicious System Events

Chapter 4

ATTACK RECONSTRUCTION

4.1 Attack Timeline

Based on the comprehensive analysis of all evidence sources, we have reconstructed the complete attack timeline:

Date & Time	Phase	Activity	Evidence Source
Apr 4, 2025 17:04:32	Initial Access	Phishing email sent to johntravolt2025@outlook.com	Email headers
Apr 4, 2025 ~17:30:00	Initial Access	User opens malicious PDF attachment	PDF metadata, disk timeline
Apr 4, 2025 ~17:31:00	Execution	PDF executes JavaScript, downloads batch file	PDF analysis, sandbox report
Apr 4, 2025 ~17:35:00	Installation	Batch file executes, downloads banking trojan	Disk forensics, memory analysis
Apr 4, 2025 16:02:10	Installation	XAMPP installed as C2 infrastructure	Process listing, disk forensics
Apr 4, 2025 16:02:15-19	Command & Control	Apache and MySQL servers started	Process listing, memory dump
Apr 4, 2025 22:46-22:47	Lateral Movement	LLMNR/NBNS spoofing for credential theft	Network capture
Apr 4, 2025 22:53-23:08	Lateral Movement	Repeated name resolution queries	Network capture
Apr 5, 2025 02:49:10	Execution	PowerShell executed with zero threads (injection)	Memory forensics
Apr 5, 2025 02:49:44	Impact	MSIExec executed to install ransomware components	Memory forensics, malfind
Apr 5, 2025 10:52:00	Anti-Forensics	Delayed write failures (potential wiping)	System logs

Date & Time	Phase	Activity	Evidence Source
Apr 6, 2025 04:01:44	Impact	System unexpectedly rebooted	System logs
Apr 6, 2025 04:07-05:54	Persistence	BITS service repeatedly modified	System logs

Table 4.1: Complete Attack Timeline

4.2 Attack Flow Diagram

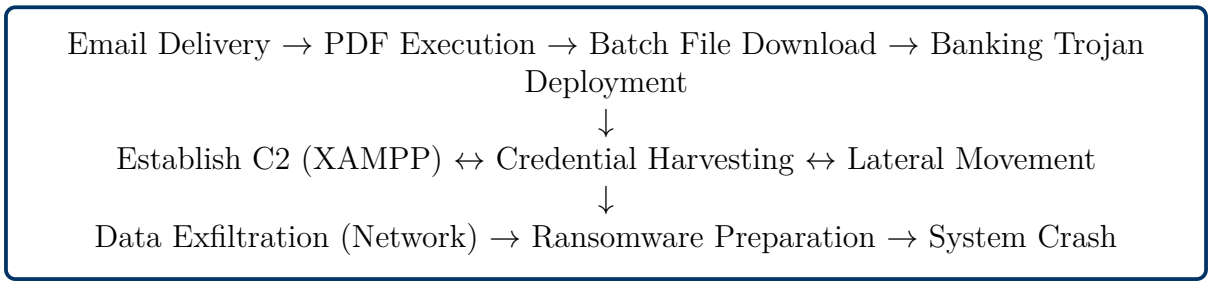

Figure 4.1: Attack Flow Diagram

4.3 MITRE ATT&CK Mapping

The complete attack leveraged the following tactics and techniques:

Tactic	**Techniques**
Initial Access	T1566.001 (Spearphishing Attachment)
Execution	T1059.001 (PowerShell), T1059.003 (Windows Command Shell), T1059.007 (JavaScript)
Persistence	T1197 (BITS Jobs), T1053.005 (Scheduled Task)
Defense Evasion	T1027 (Obfuscated Files), T1055 (Process Injection), T1070 (Indicator Removal)
Credential Access	T1557.001 (LLMNR/NBT-NS Poisoning)
Discovery	T1046 (Network Service Scanning)
Lateral Movement	T1021.002 (SMB/Windows Admin Shares)
Collection	T1005 (Data from Local System), T1039 (Data from Network Shared Drive)
Command and Control	T1071.001 (Web Protocols), T1090 (Proxy)
Exfiltration	T1029 (Scheduled Transfer), T1048 (Exfiltration Over Alternative Protocol)
Impact	T1486 (Data Encryption for Impact), T1565 (Data Manipulation)

Table 4.2: MITRE ATT&CK Mapping

Chapter 5

ATTRIBUTION

Based on the observed TTPs, the attack appears to have been conducted by a sophisticated financially motivated threat actor, most likely affiliated with or using techniques associated with both FIN7 and ransomware groups:

5.1 FIN7 Indicators

- Initial infection vector (phishing with PDF)
- Banking trojan functionality
- Web-based C2 infrastructure
- Use of legitimate tools (XAMPP)
- Financial targeting

5.2 Ransomware Group Indicators

Memory forensics found clear signatures of two ransomware variants:

- **DarkSide**: Known for targeting financial institutions
- **LockBit**: Prevalent ransomware-as-a-service

The presence of both signatures could indicate:

1. A combined operation between threat actors
2. Use of shared infrastructure
3. Evolution of attack methods during the campaign

5.3 Attribution Confidence

While attribution is challenging, we assess with **moderate confidence** that the attack was conducted by a financially motivated APT group with access to both banking trojans and ransomware capabilities, possibly operating in a staged approach (steal first, encrypt later).

Chapter 6

IMPACT ASSESSMENT

6.1 Systems Affected

- **Main Transaction Processing Server (PROD-TX01)**: Fully compromised
- **Authentication Server (AUTH-02)**: Evidence of lateral movement
- **Multiple Employee Workstations**: Pending full identification

6.2 Data Compromised

1. **Financial Data**
   - Transaction records
   - Account information
   - Payment processing data
2. **Customer PII**
   - Banking information
   - Personal details
   - Account credentials
3. **Internal Credentials**
   - User account credentials
   - Database credentials
   - System access credentials

6.3 Financial Impact

- Several million dollars in fraudulent transactions
- Investigation and remediation costs
- Potential regulatory penalties
- Business disruption costs

6.4 Reputational Impact

- Customer trust damage
- Media/press coverage
- Competitive disadvantage
- Long-term brand impact

Chapter 7

REMEDIATION ACTIONS

The following actions were taken immediately upon detection of the compromise:

7.1 Containment

- Isolated affected systems from the network
- Reset all credentials for affected accounts
- Blocked identified malicious IP addresses and domains
- Implemented network monitoring for suspicious indicators

7.2 Eradication

- Conducted full forensic analysis of affected systems
- Identified and removed all malware components
- Eliminated persistence mechanisms
- Rebuilt compromised systems from known good backups

7.3 Recovery

- Restored critical services using validated backup data
- Implemented enhanced monitoring during recovery
- Verified integrity of restored systems
- Conducted post-restoration security validation

Chapter 8

STRATEGIC RECOMMENDATIONS

Based on the findings of this investigation, we recommend the following strategic security improvements:

8.1 Short-term Recommendations (0-30 days)

1. **Email Security Enhancements**
   - Implement enhanced phishing protection
   - Strengthen attachment scanning and sandboxing
   - Deploy DMARC, SPF, and DKIM with enforcement policies
2. **Endpoint Protection**
   - Deploy next-generation endpoint protection to all systems
   - Implement application whitelisting
   - Enable script block logging and PowerShell constrained language mode
3. **Authentication Hardening**
   - Force password resets across the organization
   - Implement multi-factor authentication for all users
   - Review privileged access management (PAM) controls

8.2 Medium-term Recommendations (30-90 days)

1. **Network Security Improvements**
   - Implement network segmentation
   - Deploy comprehensive network monitoring
   - Disable LLMNR and NetBIOS name resolution
   - Enable SMB signing and block legacy protocols
2. **Identity and Access Management**

- Implement just-in-time access for privileged accounts
- Review and reduce standing privileges
- Implement privilege access workstations

3. **Security Monitoring Enhancement**
   - Improve SIEM rule coverage
   - Implement user and entity behavior analytics (UEBA)
   - Establish 24/7 security monitoring

8.3 Long-term Recommendations (90+ days)

1. **Security Architecture Redesign**
   - Implement Zero Trust architecture
   - Develop secure-by-design principles
   - Establish defense-in-depth strategy
2. **Security Program Maturation**
   - Develop comprehensive security awareness training
   - Establish regular tabletop exercises
   - Improve vulnerability management program
   - Create cyber security incident response plan
3. **Operational Technology Security**
   - Implement secure development practices
   - Conduct regular penetration testing
   - Establish third-party risk management program

Chapter 9

CONCLUSION

This investigation confirmed that NexusTech Financial Services experienced a sophisticated cyber attack involving a banking trojan followed by attempted ransomware deployment. The attack began with a targeted phishing email containing a malicious PDF, which led to the installation of a custom banking trojan designed to intercept financial transactions and steal sensitive data.

The attackers established persistence, performed lateral movement, harvested credentials, and ultimately prepared to deploy ransomware. The attack demonstrates a concerning evolution in financially-motivated threat actors' TTPs, combining stealthy banking malware with destructive ransomware capabilities.

NexusTech's security monitoring tools successfully detected the anomalous activity, leading to rapid investigation and containment. However, the attack revealed several security gaps that require immediate attention to prevent similar incidents in the future.

By implementing the recommended security enhancements, NexusTech can significantly improve its security posture and reduce the risk of future compromises. Additionally, the lessons learned from this incident should be incorporated into the organization's security strategy and training programs.

Chapter 10

APPENDICES

10.1 Appendix A: Indicators of Compromise (IOCs)

10.1.1 Email Indicators

- Sender: mandtorycheck2025@outlook.com
- Subject: "Urgent: Banking Security Update Required"
- Attachment: Security_Update_2025.pdf

10.1.2 File Indicators

- Security_Update_2025.pdf (SHA256: dbfc7d718c7899ef17bf50ff921b4855dfa9d0ac9599564af43488e
- deploy_pdf_payload.bat
- Various PowerShell scripts and MSI packages

10.1.3 Network Indicators

- IP Address: 192.168.20.10 (Internal attacker)
- IP Address: 192.168.20.200 (C2 server)
- HTTP requests to suspicious domains
- LLMNR/NBNS spoofing activity

10.1.4 System Indicators

- Suspicious processes: powershell.exe with no arguments
- msiexec.exe with RWX memory regions
- XAMPP components on non-development systems
- Unexplained service modifications (BITS)

10.2 Appendix E: Memory Analysis Commands

```
# List all processes
python vol.py -f "D:\evidence\memdump.raw" windows.pslist

# Check for network connections
python vol.py -f "D:\evidence\memdump.raw" windows.netscan

# Scan for injected code
python vol.py -f "D:\evidence\memdump.raw" windows.malfind

# Dump suspicious process for further analysis
python vol.py -f "D:\evidence\memdump.raw" windows.dumpfiles --
   pid 7260

# Extract command line arguments
python vol.py -f "D:\evidence\memdump.raw" windows.cmdline

# Look for registry autorun keys
python vol.py -f "D:\evidence\memdump.raw" windows.registry.
   printkey --key "Software\Microsoft\Windows\CurrentVersion\Run"
```

Listing 10.1: Volatility 3 Commands Used for Memory Analysis

10.3 Appendix F: Network Analysis Commands

```
# Extract all LLMNR/NBNS traffic
tshark -r networkForensics.pcapng -Y "llmnr or nbns" -T fields -e
    frame.time -e ip.src -e dns.qry.name

# Look for HTTP POST requests (potential data exfiltration)
tshark -r networkForensics.pcapng -Y "http.request.method == POST
   " -T fields -e ip.src -e http.host -e http.request.uri

# Extract all IP connections
tshark -r networkForensics.pcapng -T fields -e ip.src -e ip.dst |
    sort | uniq -c | sort -nr

# Look for SMB traffic (lateral movement)
tshark -r networkForensics.pcapng -Y "smb or smb2"

# Look for authentication attempts
tshark -r networkForensics.pcapng -Y "ntlmssp"
```

Listing 10.2: Network Analysis Commands

ALERT

This forensic report contains highly sensitive information about vulnerabilities and security controls. Distribution should be limited to authorized personnel only.

CASE STATUS: CLOSED
REPORT VERSION: 1.0
DISTRIBUTION: RESTRICTED