Incident Response Project Pitch

Phishing-Driven Compromise & Lateral Movement Investigation

HealthSecure Systems (HSS)

Incident ID: 2025-HSS-IR-002

Wayne Howlett

Cybersecurity Incident Response Analyst

Executive Incident Overview

HIGH

Phishing → PowerShell Malware → Credential Harvesting → Lateral Movement

Affected Systems

- Finance Workstation-23
- HR Payroll SQL Server
- DevAppServer (DMZ)
- Active Directory Credentials

Business Risks

- Payroll & PII exposure
- Credential compromise
- Operational disruption
- Regulatory & reputational risk

Executive Summary

A phishing-driven compromise originating from a Finance department workstation resulted in malicious PowerShell execution, outbound communication with suspicious infrastructure, and attempted lateral movement toward sensitive internal systems.

Organization & Critical Environment

Organization Overview

HealthSecure Systems is a regional healthcare software provider supporting clinics and hospitals across the Midwest. The organization stores sensitive payroll information, healthcare-related assets, and personally identifiable information.

Security Infrastructure

- Snort IDS
- Zeek Network Monitoring
- Bitdefender EDR
- Segmented Finance, HR, IT, Dev environments
- No centralized SIEM platform

Critical Infrastructure

- Workstation-23
- HR-SQL01
- DomainController1
- DevAppServer
- VPN-Gateway1

Environment Flow

Initial Attack Vector — Phishing

Phishing Email Details

From: HR-Payroll@healthsecuresystems.com

Subject: Urgent: Q1 Payroll Adjustment File

Malicious Link

hss-payroll.secure-download.com/q1-update.xlsx

Social Engineering Techniques

- Payroll urgency
- HR impersonation
- Deadline pressure
- Trusted internal communication theme

Investigation Findings

The attacker used a spoofed payroll-themed phishing email to convince the recipient to access a malicious link, leading to PowerShell malware execution and initial compromise of Workstation-23.

Attack Progression & Timeline

Attack Chain

Phishing Email ▸ Link Accessed ▸ PS Payload ▸ Cred Harvest ▸ Outbound C2 ▸ SMB/RDP/SSH

Key Timeline Events

Time	Event
01:24 AM	PowerShell payload executed
01:24 AM	PsExec service installed
01:25 AM	SMB/RDP attempts to HR-SQL01
01:25 AM	Outbound connection to 45.77.33.88
01:26 AM	SSH attempt to DevAppServer
02:11 AM	Honeypot alert triggered

The attacker rapidly progressed from phishing-based compromise to attempted lateral movement targeting payroll infrastructure and development systems.

Credential Harvesting & IoCs

Key Indicators of Compromise

- maliciousdomain.xyz
- secure-download.com
- 45.77.33.88
- PsExecsvc
- Invoke-WebRequest
- payload.ps1

Credential Abuse Findings

- Cached credentials for former employee "jcampbell"
- SSH attempt to DevAppServer
- Credential harvesting indicators identified

Security Concerns

- Stale employee accounts
- Unauthorized access attempts
- Increased privilege escalation risk
- Lateral movement toward critical systems

Root Cause Analysis & Security Gaps

Root Cause: **Successful phishing attack targeting a Finance employee.**

Contributing Security Weaknesses

- No centralized SIEM
- Manual employee offboarding
- Stale Active Directory accounts
- Inconsistent PowerShell logging
- Limited Linux monitoring
- Outdated IR playbook
- No recent phishing simulations

Investigation Conclusion

Weak identity management, incomplete monitoring visibility, and limited incident response preparedness allowed the attacker to establish an initial foothold and attempt lateral movement across the environment.

Containment, Eradication & Recovery

Containment

- Isolated Workstation-23
- Blocked malicious infrastructure
- Restricted SMB, RDP, and SSH traffic
- Reset affected credentials

Eradication

- Removed malicious PowerShell payloads
- Reimaged compromised workstation
- Removed stale employee accounts
- Conducted enterprise-wide IoC scans

Recovery

- Restored systems from trusted baselines
- Validated endpoint integrity
- Increased monitoring on critical systems
- Continued forensic review for persistence

All containment, eradication, and recovery actions were executed within the first operational period. No confirmed evidence of data exfiltration was identified during forensic analysis.

Lessons Learned & Strategic Improvements

Lessons Learned

- A single phishing email can escalate rapidly
- Weak credential management increases risk
- Incomplete visibility creates investigative blind spots
- Lateral movement can occur within minutes

Strategic Improvements

- Deploy centralized SIEM
- Enforce MFA
- Automate employee offboarding
- Improve endpoint visibility
- Conduct phishing awareness training
- Perform quarterly tabletop exercises

Long-Term Goal

Transition HSS from a reactive security posture toward a proactive, visibility-driven cybersecurity strategy.

Final Recommendations

Priority Recommendations

- Deploy centralized SIEM monitoring
- Implement MFA across critical systems
- Standardize PowerShell logging
- Expand Linux EDR coverage
- Automate identity lifecycle management
- Improve network segmentation
- Conduct recurring phishing simulations

Expected Benefits

- Faster incident detection
- Reduced credential theft risk
- Improved visibility into attacker activity
- Reduced lateral movement opportunities
- Stronger organizational resilience

Implementation of these recommendations will significantly reduce the organization's attack surface and improve the security team's ability to detect, contain, and respond to future incidents.

Conclusion

Investigation Summary

The investigation determined that a phishing-driven compromise resulted in malicious PowerShell execution, credential harvesting activity, and attempted lateral movement toward sensitive payroll and development infrastructure.

Final Outcome

- Compromised systems isolated and remediated
- Malicious infrastructure blocked
- No confirmed widespread compromise identified
- Long-term improvements recommended

Closing Statement

This incident demonstrated the importance of proactive cybersecurity practices, centralized visibility, strong identity management, and continuous incident response preparedness in defending against modern phishing-driven attacks.

Questions?

Wayne Howlett

Cybersecurity Incident Response Analyst