INCIDENT RESPONSE REPORT

Executive Summary

On **12 March 2025** , a **phishing incident** was detected on a Windows endpoint within the lab environment. The incident involved a malicious email that led to **unauthorized PowerShell execution**, simulating a common real-world phishing attack scenario.

The incident was identified through abnormal process execution and suspicious outbound network connections. Immediate containment actions were taken to prevent further compromise. Forensic analysis was conducted to determine the scope, impact, and attacker behavior.

No data exfiltration was confirmed. The incident was successfully contained, systems were recovered, and mitigation measures were implemented to prevent recurrence.

Incident Overview

Field	Details
Incident Type	Phishing Attack
Detection Method	Endpoint monitoring & log analysis

Affected System	Windows Endpoint
Severity	Medium
Status	Contained and Resolved

Incident Description

The incident began when a user interacted with a **phishing email**, leading to the execution of malicious PowerShell commands. This simulated attacker behavior typically observed after phishing attacks, including command execution and network communication attempts.

The attack did not involve privilege escalation or confirmed data exfiltration but demonstrated **post-phishing execution techniques**.

Timeline of Events

Time	Event
T0	Phishing email delivered to user
T1	User interaction triggered PowerShell execution
T2	Suspicious process activity detected

T3	Outbound network traffic observed
T4	Incident identified and escalated
T5	Endpoint isolated (containment)
T6	Forensic artifacts collected
T7	System cleaned and restored
T8	Incident closed

Detection & Analysis

Indicators of Compromise (IOCs)

- Unauthorized PowerShell execution
- Suspicious parent-child process relationships
- Unexpected outbound network connections

Analysis Performed

- Process creation analysis
- Network activity review
- Log and artifact examination

Attacker behavior was consistent with **phishing-induced command execution**.

Containment Actions

Immediate actions taken:

- Isolated affected endpoint from the network
- Terminated suspicious processes
- Blocked suspicious outbound connections

These steps prevented lateral movement and further exploitation.

Eradication & Recovery

Eradication

- Removed malicious scripts and artifacts
- Verified no persistence mechanisms existed

Recovery

- Restored normal system operations
- Reconnected endpoint to the network after validation
- Monitored system for recurring indicators

Mitigation & Prevention Steps

Area	Mitigation

Email Security	Improve phishing email filtering
Endpoint Security	Enable PowerShell logging and monitoring
User Awareness	Conduct phishing awareness training
Logging	Enable detailed process and command-line logging
Monitoring	Continuous endpoint and network monitoring

Lessons Learned

- Phishing remains a highly effective attack vector
- Endpoint visibility is critical for early detection
- Proper logging significantly improves investigation accuracy
- User awareness is essential in reducing phishing success

Conclusion

The simulated phishing incident was successfully detected, analyzed, and resolved using structured incident response procedures. Following the **SANS Incident Response methodology** ensured effective handling of the incident while minimizing impact. The exercise demonstrated the importance of preparedness, visibility, and response coordination.