Cypher Bank Limited

Phishing Investigation - Executive Summary

Phishing-Led Endpoint Compromise

Organisation: Cypher Bank Ltd
Cybersecurity Team: (Blue Team)
Cybersecurity Analyst: Joseph Christopher
Date: January 2026

Organisational Overview

Organisation Name:
Cypher Bank Ltd
Industry
Financial Services
Size of Organisation
Approximately 250 Employees

Business Context:
Cypher Bank Limited is a mid-size financial organisation that relies heavily on employee workstations and internal web applications to conduct daily operations, including handling sensitive customer financial information. Due to the nature of the financial sector, the organisation is a high-value target for phishing attacks, credential abuse, and unauthorised access attempts. Protecting user endpoints and monitoring network activity is therefore a critical priority for the Cyber Security Team.

Introduction

This document presents the final executive summary of a phishing led security incident simulation conducted within Cypher Bank Limited's internal environment.

The objective was to simulate a realistic credential harvesting attack, validate detection and response capabilities, and demonstrate end to end SOC investigation workflows using evidence based correlation. No alert was treated in isolation; every finding was corroborated across multiple telemetry sources

Scope of Investigation

The scope included internal email delivery, user interaction with phishing content, credential submission activity, endpoint telemetry, and network level monitoring. The focus remained strictly on detection, analysis, and response in alignment with real world Security Operation Centre, using industry standard tools.

Out of Scope of Investigation

cloud infrastructure, Mobile devices, Email gateway security tools, Third-party SaaS platforms, Full digital forensics and memory analysis.

Tools & Telemetry Sources

Telemetry sources included Sysmon for endpoint visibility, Splunk Universal Forwarder for log collection, pfSense Firewall for perimeter traffic, Suricata IDS for network threat detection, hMailServer for internal email services,

Investigation Methodology

The investigation followed structured Security Operation Centre phases: **detection**, **triage**, **correlation, investigation**, **response**, and **review**. Email telemetry identified malicious messages, which were correlated with user behaviour from GoPhish. Endpoint and network telemetry were analysed within defined time windows to validate attacker activity and rule out false positives.

Detection & Analysis Methodology

Analysis followed an evidence-based correlation approach:

- DNS queries reviewed to identify suspicious domain lookups
- Source and destination IPs validated against known activity timelines

- Port and protocol analysis used to identify encrypted outbound traffic
- Email events correlated with endpoint and network telemetry
- Time-bounded investigation ensured accuracy within the incident window

Artifacts & Response

1. Indicators of Compromise (IOCs) & Forensic Artifacts

During the investigation, multiple technical artifacts were reviewed and correlated across network, email, and endpoint telemetry.
Key artifacts included:

- **Phishing URL** accessed by affected users (identified via Suricata HTTP logs and DNS queries)
- **Source and destination IP addresses** associated with outbound connections
- **Ports and protocols** (e.g., TCP 443, DNS 53) confirming command-and-control style communication
- **Email sender domain and internal sender identity** observed via mail server logs
- **Endpoint execution evidence** from Sysmon logs (process creation, network connections).

  These artifacts were validated through cross-correlation in Splunk to avoid reliance on a single alert. Evidence-based correlation of DNS queries, IP addresses, ports, source/destination traffic, email events, and endpoint telemetry within a defined time window to validate phishing activity end-to-end. No alert was trusted in isolation.

MITRE ATT&CK; Mapping

Observed techniques were mapped to the **MITRE ATT&CK;** framework to standardise classification and reporting.

- **T1566** – Phishing
- **T1071.004** – Application Layer Protocol (**HTTPS**)

No evidence of execution, persistence, or lateral movement techniques was observed.

Response & Containment Actions (What Was Done)

Upon confirmation of credential harvesting activity, the following actions were taken:

- Impacted user accounts were **secured and credentials reset**
- **Active sessions revoked** to prevent further access
- Email activity reviewed to confirm **no forwarding rules or mailbox abuse**
- Endpoint activity reviewed to confirm **no malicious payload execution**
- Continued monitoring enabled for affected users and IPs
- phishing awareness reinforcement

No lateral movement or post-exploitation activity was observed.

Mitigation & Hardening Measures

Post-incident mitigation focused on preventing recurrence:

- **Multi-Factor Authentication (MFA)** enforced using conditional access controls
- Improved visibility through tighter log correlation across email, endpoint, and network sources
- User awareness reinforced around phishing identification and reporting
- Containment of impacted accounts, validation of endpoint integrity, and review of credential exposure.
- Detection dashboards were refined, logging coverage was verified, and internal awareness controls were reinforced to reduce future risk.

i

Playbooks, Process & Operational

The investigation followed a structured SOC workflow aligned with industry practice:

- Detection → Triage → Correlation → Investigation → Response → Review
- Steps reflect a **repeatable incident response playbook**
- Manual correlation was used in place of SOAR automation, but the workflow is automation-ready for future scaling

MTTR & SOC Response

Mean Time to Detect (MTTD): Minutes after user interaction
Mean Time to Investigate (MTTI): 40 minutes
Mean Time to Respond (MTTR): Same operational window

Lessons Learned & Control Improvements

Key lessons align with **NIST CSF** principles:

- **Identify:** Visibility into email, endpoint, and network telemetry is critical
- **Protect:** MFA and email authentication controls reduce blast radius
- **Detect:** Correlation across data sources increases confidence
- **Respond:** Fast containment prevents escalation
- **Recover:** Monitoring and process improvement close the loop

Recommendations & Future Improvements

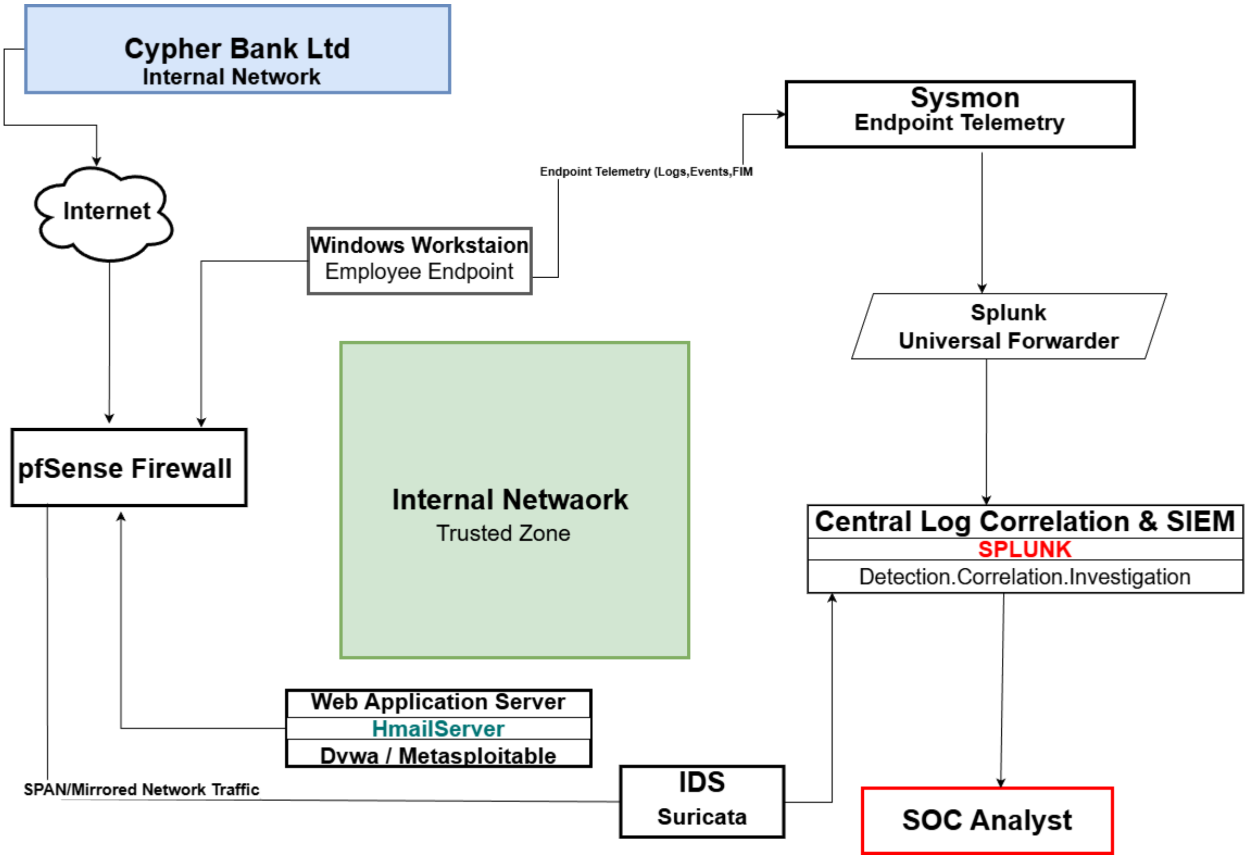
- Implement enterprise email authentication controls (SPF, DKIM, DMARC) in a production environment
- Introduce conditional access and MFA for user email access
- Formalize incident response playbooks and escalation procedures
- Enhance automated alert correlation to reduce MTTR

Final Summary

This project demonstrates Cypher Bank Ltd, InfoSec Team capability to detect, investigate, and respond to phishing threats using industry standard tools. The investigation was evidence driven, methodical, and aligned with professional SOC best practices.

Architecture Diagram

The architecture diagram illustrates the complete telemetry and investigation flow.


Cypher Bank Ltd
Internal Network
Internet
Windows Workstaion
Employee Endpoint
Endpoint Telemetry (Logs,Events,FIM
Sysmon
Endpoint Telemetry
Splunk
Universal Forwarder
pfSense Firewall
Internal Netwaork
Trusted Zone
Central Log Correlation & SIEM
SPLUNK
Detection.Correlation.Investigation
Web Application Server
HmailServer
Dvwa / Metasploitable
SPAN/Mirrored Network Traffic
IDS
Suricata
SOC Analyst