

## INC-2025-000124: [CRITICAL] Phishing Email campaign

Status: Active (Under Investigation)

Target: Finance Department (Multiple Users)

Timestamp: 2025-02-04 10:32:45 UTC

### Indicators of Compromise (IoC)

Indicator	Value
Hashes	d41d8cd98f00b204e9800998ecf8427e
Domains	secure-payments-verification[.]com (Who is lookup)
IPs	192.168.56.12 (C2 Server)
Emails	billing-alert@secure-payments-verification[.]com (Timeline)

### Impact Assessment

Indicator	Value
Users Impacted	6
Devices Impacted	3 (laptops)
Data Loss	Financial statements leaked (4GB exfiltrated)
Credential Theft	2 users
Expected Downtime	3-6 hours for remediation

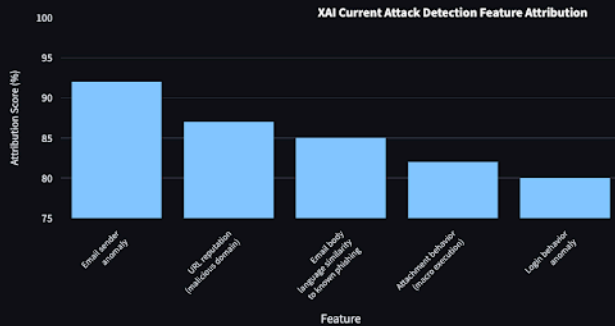
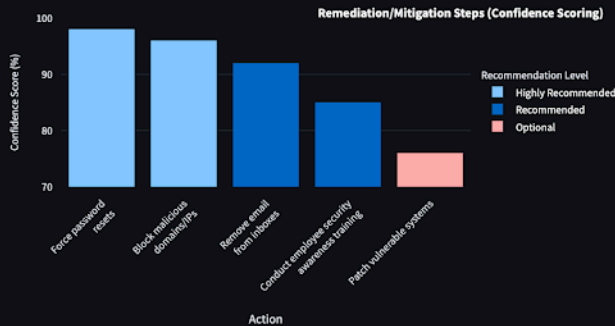
### Key Analysis

- Attack Vector: Spear-phishing email with a malicious attachment (invoice.pdf.exe)
- Payload: Remote Access Trojan (RAT)
- Campaign Name: "Invoice Payment Reminder - Urgent Action Required"
- Exploited Weakness: Lack of MFA and employees clicking on malicious links
- Simplified Investigation:
  - 6 users in the finance team opened the phishing email.
  - 2 users entered credentials on a fake login page.
  - The malicious attachment executed a PowerShell script, initiating a connection to a Command-and-Control (C2) server.
  - The infected machine exfiltrated financial reports (4GB).

### Mitigation Steps

- Isolate Impacted Devices
- Disable Compromised Accounts & Reset Passwords
- Block IoCs at Network & Endpoint Levels
- Notify Affected Users & Security Operations Center (SOC)
- Enable MFA on All High-Risk Accounts

### Explainable AI Graphs



### LLM Contextual Analysis

You: contextual analysis of the incident

LLM:

- Previous similar phishing attack: Finance\_Dept\_Phish\_2024-12-10
- Common Indicators: Email template matches 84% with prior attacks.
- Similar past target: HR & Finance users.
- Attack trend: Increasing sophistication in social engineering tactics.

You: What is the estimated financial impact of this attack?

LLM:

The estimated financial impact includes direct losses from unauthorized transactions, potential regulatory fines, and remediation costs. Additionally, reputational damage and lost productivity contribute to overall financial strain.

Would you like a deeper analysis of the financial impact?