Hybrid security consults

week 5 practical Task

Phishing Incident Report – Overdue Invoice (Emotet)

Analyst: Oni Victor
Role: Tier 1 SOC Analyst
Department Affected: Accounting
Incident Type: Phishing Email / Malware Delivery
Severity: High
Status: Confirmed (True Positive)

Executive Summary

*An employee from the Accounting department reported a suspicious email claiming an overdue invoice. Analysis of the email headers, body content, embedded link, and attachment confirmed this was a phishing attack delivering **Emotet malware**, a well-known Trojan downloader. The email failed SPF and DMARC checks, used look-alike domains, and contained a malicious ZIP attachment confirmed by VirusTotal.*

Email Overview

- **Subject:** URGENT: Overdue Invoice [9A8B]
- **Sender Display Name:** Finance Corp
- **From Address:** info@finance-corp.com
- **Reply-To:** finance.dept.22@gmail.com
- **Attachment:** invoice_9A8B.zip

1. **Header Analysis Findings.**
    a) Header fields that prove this is malicious
    Several email header indicators confirm this is a phishing email

1. **SPF Failure**
    spf=fail (domain of postmaster@finance-corp.com does not designate 198.51.100.10 as

permitted sender)
The sending IP is **not authorized** to send email on behalf of finance-corp.com.

2. **DMARC Failure**

dmarc=fail (action=reject)

- DMARC failure means the email **failed authentication checks** and should not be trusted.

3. **Suspicious Return-Path**
Return-Path: <postmaster@f!nance_c0rp.com>

Uses **character substitution** (! instead of i, 0 instead of o) → classic phishing technique.

4. **Reply-To Mismatch**

Reply-To: finance.dept.22@gmail.com
Legitimate finance departments **do not use free Gmail addresses**.

5. **Domain Mismatch**

From: info@finance-corp.com
Reply-To: finance.dept.22@gmail.com

- From and Reply-To domains do not match → strong phishing indicator.

b) Attacker's real IP address.

Received: from mail-server.company-r-us.xyz (198.51.100.10)
Attacker IP Address:
198.51.100.10

2. Body & Link Analysis.

a) **Social Engineering Technique.**

The attacker used **urgency and financial pressure**, targeting Accounting personnel.

- "**URGENT: Overdue Invoice**"
- "**30 days overdue**"
- "**Failure to pay will result in service suspension**"

This is a **Business Email Compromise (BEC) / Invoice fraud** lure designed to panic accounting staff into clicking quickly.

b) Embedded Link

- **Actual URL:**
Displayed text:

Click Here to View Your Account.

Actual link:
http://portal.finance-corp-login.com/login.php

Also visible obfuscation:

href="[http://portal.f!nance_c0rp-login.com/login.php]

c) Does the URL look legitimate?

No, it is not legitimate, because:

Uses a **look-alike domain** (finance-corp-login.com)
Real companies do **not append "-login"** to their domain
Uses **HTTP instead of HTTPS**
Uses character substitution (!,0)
Hosted on a domain unrelated to the real company

4. ***Attachment & Malware Analysis***
   Attachment Name: invoice_9A8B.zip

SHA256 Hash:

a8f5d021f1f807f7c50a1532f11f8e170a7b4de8a0f0a20f92b676f2d8a45B9C

Virus Total Detection:

- **Detections:** 52 / 68 engines
- **Malware Family:** Emotet
- **Type:** Trojan / Downloader

Risk: Credential theft, malware propagation, lateral movement

Malware Type:
Emotet Trojan (Downloader malware)

Impact:

- Drops additional malware
- Credential theft
- Email harvesting
- Lateral movement inside networks

5. Indicators of Compromise (IoCs)

a.) ***malicious IP Address***
198.51.100.10

b.) ***Malicious Domains***
portal.finance-corp-login.com
portal.f!nance_c0rp-login.com
mail-server.company-r-us.xyz

c.) Malicious File Hash (SHA256)

a8f5d021f1f807f7c50a1532f11f8e170a7b4de8a0f0a20f92b676f2d8a45B9C

Malicious Sender / Email Artifacts
Return-Path: postmaster@f!nance_c0rp.com
Reply-To: finance.dept.22@gmail.com

5. Final Recommendation:

a) True Positive or False Positive?
TRUE POSITIVE
This is a confirmed **phishing email delivering Emotet malware**.
Threat Level: High

b) Immediate next steps (Tier 1 Analyst actions)

Actions Taken & Recommendations
Immediate Actions

1. Quarantine the email across all mailboxes
2. Block malicious IPs, domains, and hash values
3. Confirm the attachment was not opened

Confirmed.

- Isolate the affected endpoint
- Escalate to Tier 2 SOC
- Initiate malware incident response procedures

Preventive Measures

- Security awareness reminder to Accounting department
- Update email filtering rules
- Add IoCs to SIEM detection rules

Conclusion.

This incident demonstrates a classic financial-themed phishing attack delivering Emotet malware. Prompt user reporting and SOC analysis prevented potential compromise. Continued awareness training and technical controls are recommended to reduce future risk.

- **Report Prepared By:** Oni Victor
  SOC Tier 1 Analyst