ATHANASIUS J.K GADOSEY

Week 5

Practical Task: The Urgent Invoice

1. **Header Analysis**

   Header fields that show this is malicious:

   - **SPF failed** because the sending IP was **not authorized** to send email on behalf of the claimed domain.
   - **DMARC failed:** The domain's email protection policy failed.
   - **Return-Path mismatch:** *postmaster@f!nance_c0rp.com* uses look-alike characters, which is a common phishing trick.
   - **Reply-To mismatch:** Upon reviewing the message, it appears that this reply was sent to a Gmail address rather than a corporate finance domain.

   - **Attacker's real IP address:** *198.51.100.10*, as shown in the received header, this was the actual server.

2. **Body and Link Analysis**

   Social engineering tactic used:

   - **Fear and urgency-** It was claiming an overdue invoice and threatening service suspension to pressure the victim into acting quickly.

   Actual URL in the email:

   http://portal.f!nance_c0rp-login.com/login.php

   Does this URL look legitimate? Why or why not?

   - No. The domain uses typosquatting (*f!nance_c0rp* instead of *finance-corp*) and is not the real company domain therefore making it a classic phishing login page meant to steal credentials.

3. **Attachment Analysis**

   Attachment name:

   - *invoice_9A8B.zip*

   Type of malware (from VirusTotal):

   - **Trojan / Downloader,** specifically flagged as **Emotet.** This type of malware is commonly used to steal credentials and also deliver additional payloads.

4. **Indicators of Compromise (IoCs)**

   IoCs to share with Tier2 / Firewall team:

   - **Sender IP:** *198.51.100.10*
   - **Malicious URL:** *portal.f!nance_c0rp-login.com/login.php*
   - **Reply-To email:** *finance.dept.22@gmail.com*
   - **Malicious hash (SHA256):** *a8f5d021f1f807f7c50a1532f11f8e170a7b4de8a0f0a20f92b676f2d8a45b9c*

5. **Final Recommendation**
   True Positive or False Positive?

   - **True Positive**
     Multiple red flags did confirm it was phishing, failed email authentication, spoofed domains, a malicious attachment and strong AV detections.

   Immediate next step as Tier 1 Analyst:

   - I will ensure the email is quarantined, confirm no one opened the attachment or clicked the link, then alert Tier 2, and block the sender IP, domain, and hash across email and network security tools.