Task2 : PHISHING EMAIL ANALYSIS REPORT

Alert: User reported phishing mail.

Description: The alert triggers in two ways one is detected by defender or any user reports any mail as phishing email.

Log sources: ESA (email securing appliance), MS 365 Defender.

Gathering information: Sender Domain, Sender mail address, URL, Source IP, Email subject, Received details.

Analysis:

- Once the alert triggered on the incident review dashboard, we will start validating the reputation of sender domaining for (e.g.: support@paypa1.com[]) and associated IP address.
- which include checking the reputation using OSINT Tool like Virus total, Abuse IP, MS Tool box, IP vault, Threat Intelligent tool.
- The MS365 Defender tool as ESA through which we will perform the complete email analysis.
- Once we login to defender under email and collaboration in explorer we can filter out the report the email by using subject line sender mail address and sender domain.
- Once we filter out the detected email, we use to open the email in a tab to perform the complete analysis.
- In analysis we will validate the sender and recipient detail followed by checking the return path and return path domain to validate whether the email is spoofing or not.
- Then we will validate the email authentication SPF, DKIM, DMARK.
- **SPF (Sender Policy Framework):** which helps to authenticated user whether mail came from the authenticated user or not by comparing to domain name to IP address.
- **DKIM (DomainKeys Identified Mail):** which help to validating the integrity of the mail to make sure the mail is not tampering while flowing to defend mail server by checking the cryptography signature.
- **DMARC (Domain-based Message Authentication, Reporting & Conformance):** Ensures policy enforcement by aligning SPF/DKIM with the sender’s domain.

- In the mean time we will do the header analysis using Microsoft message header analysis apart from this we will also validate the other entities like attachments and URL.
- Once we click detected attachments the defender will give the analysis details and we can also perform the offline analysis by capturing hash value of detected file.

Actions:

- ✓ If any negative attributes observe with the report analysis like negative email authentication domain IP reputations, attachments and URL detected.
- ✓ We create the incident to remove the mail from the all-user inbox to ESA team .
- ✓ We also removed to proxy and firewall team to block the domain and IP respectively.

Scenario:

- ✓ if any user clicked on any URL that can identified in URL clicks.
- ✓ Then we will check the user activity and with the respect to log in activity to make sure user credential has not been shared also we will write the email to user to reset the password
- ✓ If any attachment downloaded by the user we recommend EDR team or we create scan tool to check disposition of file.

FOR EXAMPLE:

Subject: Urgent! Verify Your Account Immediately

Sender: support@secure-paypal-update.com []

Body: Your account will be suspended. Click here to verify: http://paypal-update-login[.]xyz

OSINT Analysis Steps:

1. Check Sender Domain Reputation

- Use tools like VirusTotal / AbuseIPDB / Talos Intelligence.
- Result: secure-paypal-update.com flagged as malicious / phishing domain.

2. Check Associated IP Address

- Resolve domain → IP = 185.189.15.22.
- OSINT check on AbuseIPDB shows history of spam & phishing activity.

3. Analyze URL

- URL paypal-update-login[.]xyz scanned on VirusTotal → phishing redirect site imitating PayPal.

4. Check WHOIS Information

- Recently registered domain (less than 1 month).
- Hidden registrant details (often used in malicious activity).

5. Verification

- Then we will validate the email authentication SPF, DKIM, DMARK.
- Microsoft 365 Defender / Email gateway logs confirm multiple delivery attempts of this phishing mail.

Conclusion:

This email is a phishing attempt, using a fake PayPal domain to trick users into entering credentials. OSINT tools flagged the domain, IP, and URL as malicious, confirming the threat.