Phishing Email Analysis Report

1. Overview

This report documents the analysis of a suspected phishing email. The objective was to identify phishing indicators within the email headers, sender details, embedded links, attachments, and body content.

2. Email Sample Details

File: sample_phishing.eml

Date Analyzed: 2025-10-04

Source: Public phishing sample repository

3. Header Analysis

- Sender: "Microsoft Support <support@micr0soft.com>" (spoofed domain).

- Return-Path: <random@phishy-domain.net> (does not match sender).

- Received Path: Originated from an IP in a region unrelated to Microsoft.

- Authentication: SPF = Fail, DKIM = None, DMARC = Fail.

4. Link and Attachment Analysis

- Links: Displayed as 'https://paypal.com' but actually redirects to 'http://malicious-site.biz/login'.

- Attachments: 'invoice.docm' (macro-enabled Word document).

- Hash (SHA256): e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

- Likely to contain malicious macros for credential theft.

5. Email Body Analysis

- Subject: 'URGENT: Verify your account now or risk suspension.'

- Content: Threatens account closure within 24 hours if no action is taken.

- Language: Urgent and fear-inducing tone, common in phishing attacks.

- Spelling/Grammar: Several grammatical mistakes and awkward phrasing detected.

6. Indicators of Phishing

1. Spoofed sender domain (micr0soft.com).

2. Failed SPF/DKIM/DMARC authentication.

3. Mismatched URLs (paypal.com vs malicious-site.biz).

4. Suspicious macro-enabled attachment.

5. Urgent and threatening language in the message body.

6. Multiple grammar and spelling errors.

7. Recommendations

1. Do NOT click any links or open attachments in this email.

2. Block the sender domain and originating IP address.

3. Report the phishing attempt to the email provider and internal IT/security team.

4. Educate users on identifying phishing attempts and safe practices.

5. Deploy email security tools with SPF/DKIM/DMARC enforcement.

8. Conclusion

This email exhibits multiple strong indicators of phishing, including spoofed domains, failed authentication checks, malicious links and attachments, and social engineering techniques. It should be treated as a confirmed phishing attempt.