Yespanchi - Email Scan Guardian

Website: https://www.yespanchi.tech
Contact: 9360784554
Address: TM Maistry Street Extn Thiruvanmiyur Chennai

Email Security Analysis Report

File: pasted-email.eml
Generated: 15/09/2025, 16:09:17

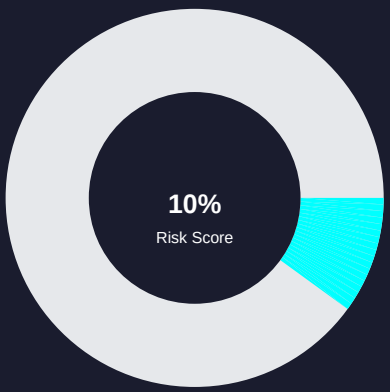
Analysis Summary

Authentication:
- SPF: pass
- DKIM: pass
- DMARC: fail or not present

Security Issues: 2 Issues

Phishing Risk: Medium (40%)

Medium	10	40%
Risk Level	Risk Score	Confidence



System Verdict: Suspicious

AI Security Analysis Report

Analysis for: tarch4.com

Security Report: benliu@tarch4.com

1. Executive Summary

This security report summarizes the analysis of an email sent from benliu@tarch4.com with the subject "pasted-email.eml". The email was found to have a DMARC policy that is not satisfied, indicating a potential security risk. Additionally, medium-risk phishing was detected, suggesting that the email may be attempting to deceive the recipient into divulging sensitive information.

2. Risk Assessment

The risk assessment for this email is classified as SUSPICIOUS due to the failure of the DMARC policy and the detection of medium-risk phishing. This suggests that the email may not be legitimate or trustworthy, and further investigation is warranted to determine its true intentions.

3. Key Security Findings

- The sender's domain (tarch4.com) has a DMARC policy that is not satisfied, indicating a potential security risk.
- Medium-risk phishing was detected in the email, suggesting that it may be attempting to deceive the recipient into divulging sensitive information.
- All authentication checks (SPF, DKIM) pass, but the DMARC result is fail or not present.
- No links or attachments were found in the email.

4. Recommendations for Further Investigation

To further investigate this email and determine its true intentions, we recommend the following:

- Verify the authenticity of the sender's domain (tarch4.com) to ensure that it is a legitimate source.
- Conduct a thorough analysis of the email's content to identify any potential phishing indicators or malicious code.
- Check for any known threat patterns or malware signatures in the email.
- Consider implementing additional security measures, such as sandboxing or isolation, to contain any potential threats.

5. Overall Verdict

Based on our analysis, we conclude that this email is classified as SUSPICIOUS due to the failure of the DMARC policy and the detection of medium-risk phishing. Further investigation is warranted to determine its true intentions and ensure the security of the recipient's systems and data.

6. Final Recommendation

In light of these findings, we strongly recommend that the recipient exercise extreme caution when interacting with this email. We suggest that they do not open any attachments or click on any links until further analysis has been conducted and the authenticity of the sender has been verified. Additionally, we recommend implementing additional security measures to contain any potential threats and protect against future attacks.