

Yespanchi - Email Scan Guardian

Website: <https://www.yespanchi.tech>

Contact: 9360784554

Address: TM Maistry Street Extn Thiruvannamipur Chennai



Email Security Analysis Report

File: pasted-email.eml

Generated: 09/09/2025, 18:24:07

Analysis Summary

Authentication:

SPF: pass

DKIM: pass

DMARC: fail or not present

Security Issues: 2 Issues

Phishing Risk: Medium (40%)

Medium

Risk Level

10

Risk Score

40%

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 categorized 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 entirely legitimate and could potentially pose a threat to the security of the recipient's systems or data.

3. Key Security Findings

- The sender domain, tarch4.com, has a SPF result of pass, indicating that the sending IP address is authorized to send emails on behalf of this domain.
- The DKIM result is also pass, confirming that the email was digitally signed using a valid key pair.
- However, the DMARC result is fail or not present, suggesting that the email's authentication may have been compromised or tampered with.
- Medium-risk phishing was detected in the email, indicating that it may be attempting to deceive the recipient into divulging sensitive information.

4. Recommendations for Further Investigation

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

- Verify the authenticity of the sender's identity by contacting them directly or checking their website.
- Check the email's content for any suspicious links or attachments that could potentially compromise your system or data.
- Run a thorough virus scan on any attachments received from this email to ensure they are free from malware.

5. Overall Verdict

Based on our analysis, we conclude that this email is SUSPICIOUS and may pose a security risk to the recipient's systems or data. Further investigation is recommended to determine its legitimacy and potential impact.

6. Final Recommendation

To mitigate the risks associated with this email, we recommend taking the following actions:

-
- Do not open any attachments or click on links from this email until its authenticity has been verified.
 - Report any suspicious activity or emails to your organization's security team for further investigation.
 - Implement additional security measures, such as two-factor authentication and regular software updates, to protect against potential threats.

By taking these precautions, you can help ensure the security of your systems and data.