Email samples and screenshots in this analysis are from Phishing Pot by Peixoto, licensed under CC BY-NC 4.0. The original sample analysed in this report can be found below:

Phishing Pot: https://github.com/rf-peixoto/phishing_pot
Peixoto: https://github.com/rf-peixoto
License: https://github.com/rf-peixoto/phishing_pot/blob/main/LICENSE
Source file: https://github.com/rf-peixoto/phishing_pot/blob/main/email/sample-5871.eml

Executive Summary
==========
This report analyzes a phishing email impersonating Ledger Solutions, sent from an unrelated Ticino email address. The attacker attempts to trick the recipient into clicking a fraudulent link in a pdf file under the pretext of updating the security of their crypto assets. Indicators of compromise include urgency tactics, technology confusion, the use of a malicious Webflow-hosted URL, and the use of a non-legitimate email address. The email demonstrates typical characteristics of credential-harvesting attempts. Defensive actions were taken to block the sender and associated domains to prevent further exposure.

Headers
==========
Date: Thu, 28 Aug 2025 04:25:58 -0600
Subject: 10 Years of Ledger: Secure Self-Custody for All

To: Recipients <whittakerjeff658@ticino.com>
From: "ledger solutions" <whittakerjeff658@ticino.com>

Reply-To: None
Return-Path: whittakerjeff658@ticino.com

Sender IP: 217.160.57.165 (IONOS, DE)
Resolve Host: proxy-5.proxy.shared.ham.xion.oxcs.net

Message-ID:
<aa6344ae-b227-4e5d-80e7-9bf912866d63@BN2PEPF000055DF.namprd21.prod.outlook.com
>

Attachments
==========
Attachment Name: Ledger Support.pdf
MD5: 22c4808f241e69dea62266334d7a4ecb
SHA1: 10d1d765279e4d927bfefd11c9b5bef7045b9d17
SHA256: a094eaf7492d5e10feabe05a4d1e9487c3ebecddd9b72382e78d82be529dcb56

URLs
==========
hxxps[://]www[.]imaservice[.]com/azienda[.]phtml
hxxps[://]www[.]immobiliarebonetti[.]com/wp-includes/IXR/userInfo/

Description
==========
The email claims to be from Ledger, which is a crypto wallet company. The email says Ledger has an AI firmware update. For more information the user should look at the attached pdf file.

There are no images or logos in the email. And an absence of standard security disclaimers or contact information that legitimate crypto companies always include

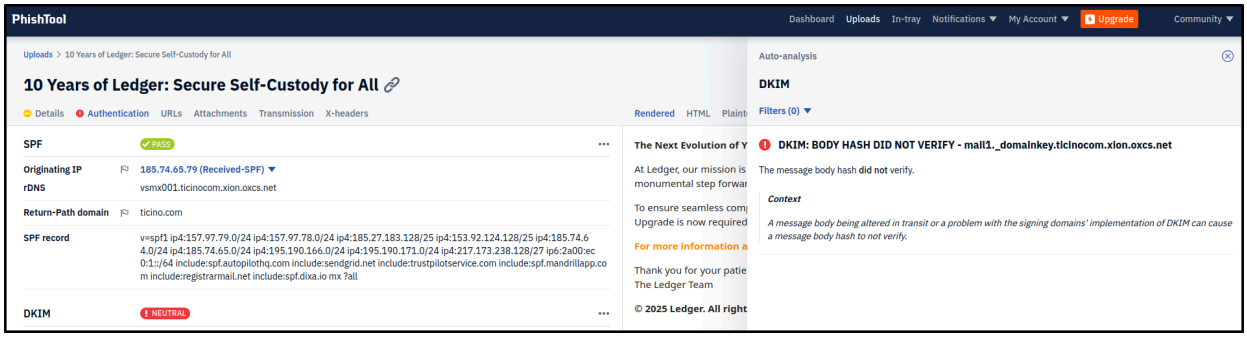
Indicator of urgency: as it involves the security of crypto assets, which can have a lot of value, they may be urged to get this update to secure their assets.

Indicator of technology confusion: AI is the latest buzzword that is ambiguous enough to make users lower their guard. The use of 'AI' exploits current hype to increase credibility.

Artifact Analysis
==========
Sender Analysis:
The sender uses the ticino[.]com domain in the From and Return-Path header, which is not affiliated with Ledger, who use the ledger[.]com domain for email communication. The From email address is also obscured using a display name and reads “ledger solutions”. The legitimate company would capitalize their name.

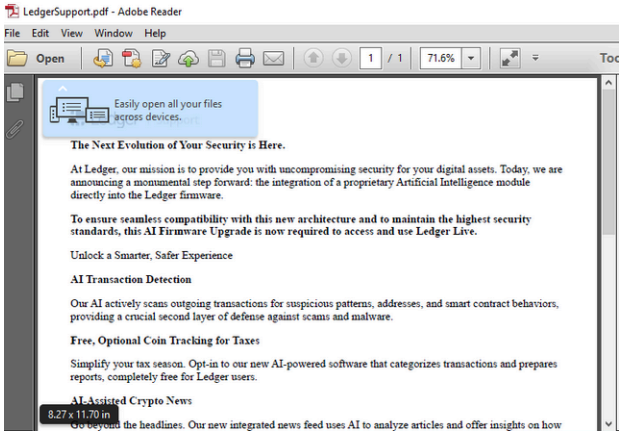
The email address used by the sender is also the exact same as the recipient’s. It is unlikely the real owner of the email address sent themselves a phishing email.

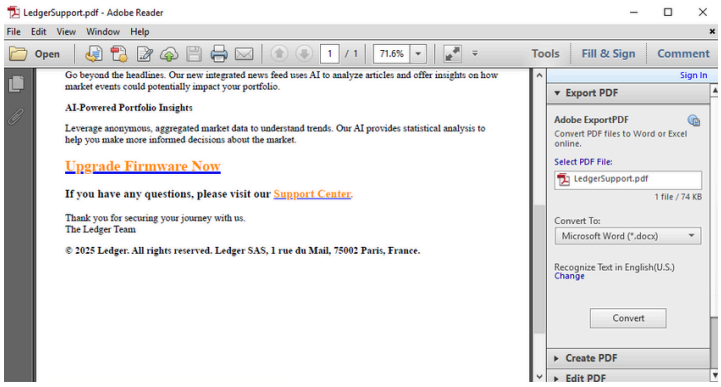
While DKIM passes according to the headers in the eml file, when using PhishTool, it says DKIM fails.



The To header was possibly changed by whoever submitted this eml file to Phishing Pot for privacy reasons. From their ReadMe, normally sensitive information is changed to phishing@pot, but the contributor may have made a mistake and copy-pasted the wrong email address in this case. As it is unclear and there is no way to find out what happened when the eml file was added to Phishing Pot, for this exercise, let's assume that the attacker used "whittakerjeff658@ticino.com", and the recipient used another unknown email address.

Attachment Analysis:
The attachment is not known to VirusTotal. For further analysis, the attachment was dumped from the eml file and uploaded to Hybrid Analysis to test it in a sandbox. The report gives it a "no specific threat" rating. The screenshots in the Hybrid Analysis report show that the pdf itself seems to just contain text and a link to "Upgrade Firmware Now".





Using a PDF parsing script, the following URL was found:
hxxps[://]www[.]imaservice[.]com/azienda[.]phtml

Pdf files are often used by attackers to bypass spam filters and because links in emails are trusted less than links in documents.

URL Analysis:

There are no hits for the URL on VirusTotal, but when doing an automatic sandbox report on Hybrid Analysis, it is deemed Malicious. The report says that the URL contacts a page called “hxxps[://]www[.]immobiliarebonetti[.]com/wp-includes/IXR/userInfo/” which Hybrid Analysis deems to be malicious. The “immobiliarebonetti[.]com” domain has 13 security vendors on VirusTotal say that it is Phishing or Malicious as well.

The screenshots in the report from Hybrid Analysis show that the redirect from the “imaservice” page to the “immobiliarebonetti” is automatic. So it looks like the attacker tried to obfuscate the eventually malicious page with the “imaservice” URL. This is an often used tactic by attackers.

Verdict
==========
Due to the sender not being affiliated with Ledger, this is a clear impersonation and spoofing attempt.

For a legitimate service, there would be no reason to hide the link to a firmware upgrade in an attached pdf file. Updates are normally rolled out automatically through the app store.

The URL in the pdf file is also not affiliated with Ledger and redirects to a domain deemed malicious by both Hybrid Analysis and VirusTotal.

As a result of the analysis, this email has been determined to be malicious.

Defense Actions
==========
After performing a message trace, no other users within the organization received an email from this sender or with a similar subject line.

To prevent the malicious sender from sending any other email to the organization, I have blocked the “whittakerjeff658@ticino.com“ email address on the email gateway. The ticino[.]com domain seems to be related to a Swiss ISP called Ticinocom, so the blocking of the entire domain is not necessary.

To ensure users are unable to access these malicious URLs or domains, I have blocked the below domains on the EDR and on the Web Proxy.
imaservice[.]com
immobiliarebonetti[.]com