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-1526.eml

Executive Summary
==========
This report analyzes a phishing email impersonating Lido, sent from an onmicrosoft[.]com email address. The attacker attempts to trick the recipient into clicking a fraudulent link under the pretext of getting free $ETH coins. Indicators of compromise include grammar issues, failure of DKIM authentication, the use of various obfuscation techniques, and of a malicious self-hosted URL. Although the phishing page has since been removed, 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, 5 Oct 2023 16:59:21 +0000
Subject: #rodrigofp: V2 Airdrop

To: phishing@pot
From: Ref.401628845@qmhs[.]onmicrosoft[.]com
Display name: Airdrop@lidoFinance

Reply-To: None
Return-Path: Ref.401628845@qmhs[.]onmicrosoft[.]com

Sender IP: 40.107.20.96 (US based, owned by Microsoft)
Resolve Host: EUR05-DB8-obe.outbound.protection.outlook.com

Message-ID:
<PAXPR10MB5686AE78149E3EF50BEF849786CAA@PAXPR10MB5686.EURPRD10.PROD.OUTLOOK.COM>

URLs
==========
hxxps[://]click[.]pstmrk[.]it/3s/aql[.]z13[.]web[.]core[.]windows[.]net%2F/ahc/rWmwAQ/AQ/a19f7661-1caa-482a-a0f1-4d0b0b35524f/1/bVMxh49_yB?/67912984rodrigofp

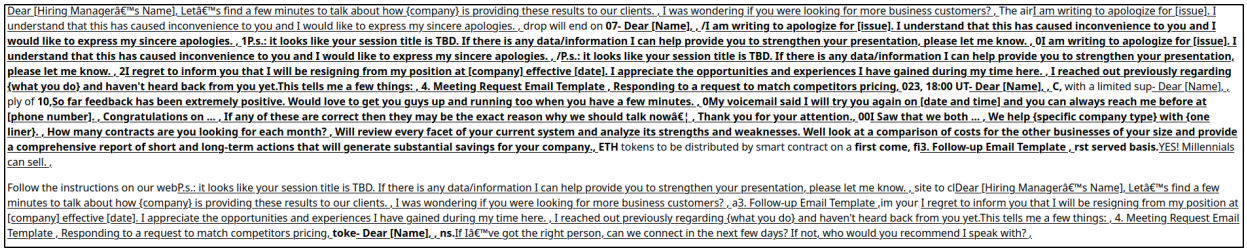
Description
==========
The email claims to be from Lido, and that the user is eligible to claim $ETH, which is a well known crypto currency. To claim the tokens, the user is urged to click on a Join Airdrop button in the email.

The email MIME body is in Base64, which in itself is not suspicious, but Base64 is often used for obfuscation purposes.

There are a number of grammar mistakes and typos. There are indicators of urgency, as the airdrop has a time limit of only 2 days.

There is text in a very small font at the bottom of the email that seems to be placeholder text completely unrelated to the rest of the email.

There is more hidden text when the email is viewed in simple HTML, also all not related to the rest of the email, with a lot of placeholder text, such as [issue], [phone number] and [Name].


Dear [Hiring Managerâ€™s Name], Letâ€™s find a few minutes to talk about how {company} is providing these results to our clients. , I was wondering if you were looking for more business customers? , The air[am writing to apologize for [issue]. I understand that this has caused inconvenience to you and I would like to express my sincere apologies. , drop will end on **07- Dear [Name]. , , /I am writing to apologize for [issue]. I understand that this has caused inconvenience to you and I would like to express my sincere apologies. , 1P.s.: it looks like your session title is TBD. If there is any data/information I can help provide you to strengthen your presentation, please let me know. , 0I am writing to apologize for [issue]. I understand that this has caused inconvenience to you and I would like to express my sincere apologies. , /P.s.: it looks like your session title is TBD. If there is any data/information I can help provide you to strengthen your presentation, please let me know. , 2I regret to inform you that I will be resigning from my position at [company] effective [date]. I appreciate the opportunities and experiences I have gained during my time here. , I reached out previously regarding {what you do} and haven't heard back from you yet.This tells me a few things: , 4. Meeting Request Email Template , Responding to a request to match competitors pricing. 023, 18:00 UT- Dear [Name], , C,** with a limited sup- Dear [Name], , ply of **10,So far feedback has been extremely positive. Would love to get you guys up and running too when you have a few minutes. , 0My voicemail said I will try you again on [date and time] and you can always reach me before at [phone number]. , Congratulations on ... , If any of these are correct then they may be the exact reason why we should talk nowâ€¦ , Thank you for your attention., 00[Saw that we both ... , We help {specific company type} with {one liner}. , How many contracts are you looking for each month? , Will review every facet of your current system and analyze its strengths and weaknesses. Well look at a comparison of costs for the other businesses of your size and provide a comprehensive report of short and long-term actions that will generate substantial savings for your company. , ETH** tokens to be distributed by smart contract on a **first come, fi3. Follow-up Email Template , rst served basis.**YES! Millennials can sell. ,

Follow the instructions on our webP.s.: it looks like your session title is TBD. If there is any data/information I can help provide you to strengthen your presentation, please let me know. , site to clDear [Hiring Managerâ€™s Name], Letâ€™s find a few minutes to talk about how {company} is providing these results to our clients. , I was wondering if you were looking for more business customers? , a3. Follow-up Email Template ,im your I regret to inform you that I will be resigning from my position at [company] effective [date]. I appreciate the opportunities and experiences I have gained during my time here. , I reached out previously regarding {what you do} and haven't heard back from you yet.This tells me a few things: , 4. Meeting Request Email Template , Responding to a request to match competitors pricing. **toke- Dear [Name], , ns.**If Iâ€™ve got the right person, can we connect in the next few days? If not, who would you recommend I speak with? ,

There is also a section about a Microsoft service agreement in this hidden text.

Artifact Analysis
==========
Sender Analysis:
The sender’s display name used three obfuscation techniques to hide that the email is from Ref.401628845@qmhs[.]onmicrosoft[.]com. It uses a display name to appear as Airdrop@lidoFinance. When looking at the raw email, it is encoded in Base64. And the A and o in the display name are using Greek letters instead of Latin letters.

The onmicrosoft[.]com domain is owned by Microsoft, but is used by its users. An onmicrosoft domain is a temporary, fallback domain provided by Microsoft when you sign up for a Microsoft 365 service.

The DKIM check failed, so the message hash did not verify. This means that either the email was altered during transit, or the DKIM signature was faked.

URL Analysis:

The URL is not related to Lido, who use lido.fi. The page being linked is no longer available and does not have any hits on VirusTotal. Pstmark[.]it currently has a page that recommends users to go to https://postmarkapp.com/ which is a legitimate website and service.

The URL mentions windows in the path section, likely trying to trick users in believing it is a legitimate link.

E-mail body analysis:
To confuse spam detection software, there is a lot of hidden text between the various words. That is likely why it looks like some spaces are missing. The text seems to be hidden by using a font size of 0. For example, what you see in the email is below:

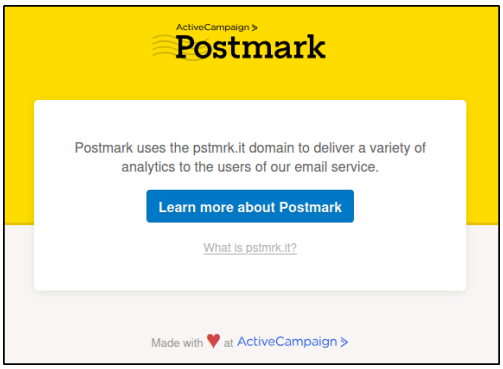
But when you select and copy the text, all of the following text is hidden:

A snapSounds interesting? , shot hasI Saw that we both ... , We help {specific company type} with {one liner}. , How many contracts are you looking for each month? , Will review every facet of your current system and analyze its strengths and weaknesses. Well look at a comparison of costs for the other businesses of your size and provide a comprehensive report of short and long-term actions that will generate substantial savings for your company., been taken on - [List of Information Needed] , I would like to express my gratitude for your assistance with [task/project]. Your contribution was invaluable and greatly appreciated. , Do you have any current issues that we can help answer? , Iâ€™m hoping you can help me, who handles the [insert pain point here] decisions at {company} and how might I get in touch with them?, **2Thank you for your patience and understanding. , 1st JThis is SDR with RJMetrics. Wanted to introduce myself, as {company}'s sales development platform looks similar to many of the businesses we work with everyday. , une 2023** I regret to inform you that I will be resigning from my position at [company] effective [date]. I appreciate the opportunities and experiences I have gained during my time here. , I reached out previously regarding {what you do} and haven't heard back from you yet.This tells me a few things: , 4. Meeting Request Email Template , Responding to a request to match competitors pricing, of all wallWishing you all the best. , ets that has been Thanks! , using our plaDear [Hiring Managerâ€™s Name], Letâ€™s find a few minutes to talk about how {company} is providing these results to our clients. , I was wondering if you were looking for more business customers? , tfoI regret to inform you that I will be resigning from my position at [company] effective [date]. I appreciate the opportunities and experiences I have gained during my time here. , I reached out previously regarding {what you do} and haven't heard back from you yet.This tells me a few things: , 4. Meeting Request Email Template , Responding to a request to match competitors pricing, rm for stThis is SDR with RJMetrics. Wanted to introduce myself, as {company}'s sales development platform looks similar to many of the businesses we work with everyday. , aking.Any

It looks like the underlined text is what is hidden, while the non-underlined text is what shows up when viewed in Original HTML

Verdict
==========
This is a clear spoofing attempt, as Lido would use their own email domain and not one from Microsoft. The attacker is also using various ways of obfuscation to avoid spam detection software.

The URL is also not related to Lido, and is currently not available. The domain is used by a legitimate service called Postmark.



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 “Ref.401628845@qmhs[.]onmicrosoft[.]com” email on the email gateway. The onmicrosoft[.]com domain is legitimate, but this particular user is malicious.

To ensure users are unable to access this malicious URL or domain, I have blocked “hxxps[://]click[.]pstmrk[.]it/3s/aql[.]z13[.]web[.]core[.]windows[.]net%2F/ahc/rWmwAQ/AQ/a19f7661-1caa-482a-a0f1-4d0b0b35524f/1/bVMxh49_yB?/67912984rodrigofp” on the EDR and on the Web Proxy. While the domain seems to now be used by a legitimate service, it is unlikely that a legitimate service will use that particular URL in the future.