Phishing Threat Investigation Cybersecurity Project

Scope: My goal in this project is to demonstrate how a cybersecurity analyst analyzes phishing emails by identifying if they are really phishing scams while using tools as my evidence and looking at the obvious signs of phishing as well. I will also investigate what threats there may be. The expected outcome is that all my phishing email samples will be detected as suspicious/malicious.

Background: Phishing Threats are a real problem around the globe which happens often and there are still active threats today. One of the most common types of phishing threats are usually by email, and they consist of suspicious/malicious emails being sent to individuals. The emails typically include convincing information, malicious attachments, and suspicious links. Their goal is to get you to click on the link or reply back with your personal details. The threat actor's motivation is to gain credentials or money from the targets. It is important to investigate these attacks as many humans fall into the trap and believe that the sender can be trusted, which causes them to click on harmful links putting them at risk. My goal as a cybersecurity analyst and phishing threat investigator is to help others mitigate this risk.

Some best practices may be to enforce Multi Factor Authentication (MFA) and deploy SPF/DKIM/DMARC rules, user reporting systems, and awareness training programs to further educate individuals on how to avoid such threats. There are also many tools to use such as Microsoft Defender for Office 365, Mimecast, Splunk SOAR, Sandboxes, VirusTotal, emlAnalyzer, etc. Many of these tools scan emails for any malicious attachments or block out spam/phishing. Tools like sandbox will isolate the environment so your own personal device is not affected if you click a link.

Analysis of threats, vulnerabilities, & security concerns:

Phishing threats come in many forms and when it comes to phishing emails attackers may spoof domains to fool others into thinking that they are from a trusted source. Vulnerabilities are high at times as recipients fall for the scams because it may sound believable or the “brand” names in the email may sound familiar to them. Also, there are vulnerabilities with lack of security awareness which many people do not have knowledge of checking before trusting a sender. Technical vulnerabilities like absent

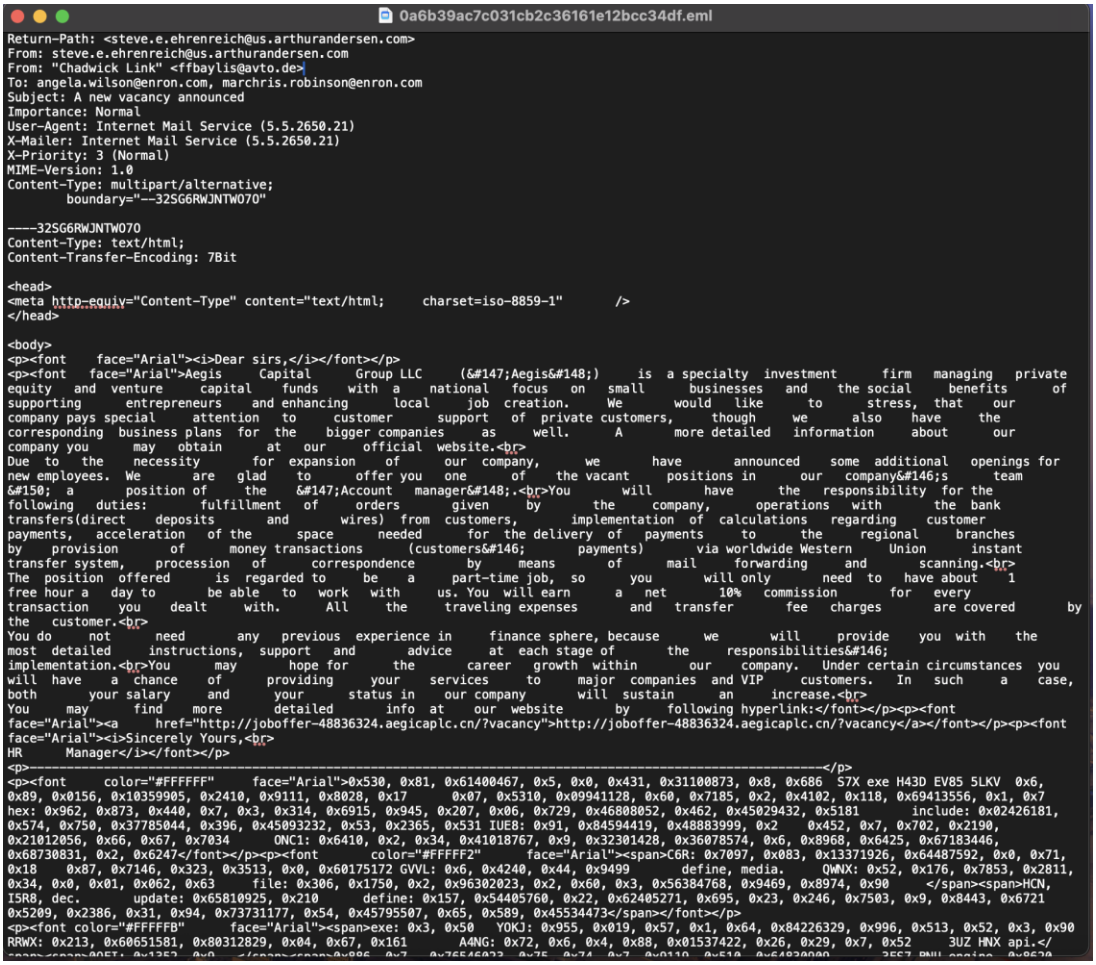
policies or inefficient email authentication protocols allow attackers to spoof email addresses. Security concerns arise when email policies such as DKIM, DMARC, and SPF are not as enforced as they should be. To ensure individuals are protected these authentication methods should be mandatory to use on all email servers.

Relevant frameworks & industry standards:

- Frameworks: MITRE ATT&CK techniques provide details about structured attacks and help others to categorize attacks. This helps industries and individuals to better understand incidents and how to respond to them. NIST CSF gives guidelines on how to identify, protect, detect, and respond to digital threats.
- Industry standards: Sender Policy Framework (SPF) – authenticates which users can send emails. Domain Keys Identified Mail (DKIM) - digital signatures applied to verify the sender. Domain Based Authentication Reporting & Conformance (DMARC) - describes how receiving senders deal with failed SPF//DKIM checks

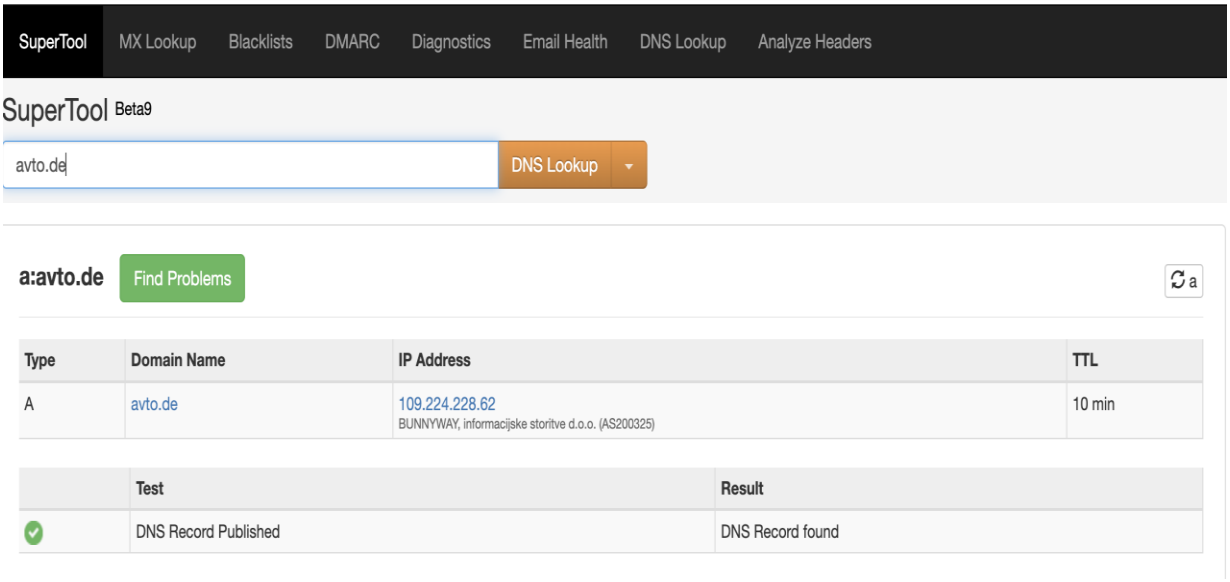
Phishing Threat Investigation Method:

My first step was to find a few phishing email samples to work on, so I used sample data from EPVME and Nazario. I started with a sample from EPVME and found the datasets on GitHub. I downloaded everything and in the folder were many eml files and I chose 2 to work on. I will now explain how I analyzed **Sample 1 from the EPVME dataset**. I hit right click on the file and open with “other” then clicked Text Editor to view the data in a more readable format. Text Editor is used for many things like viewing raw data. (image result below):

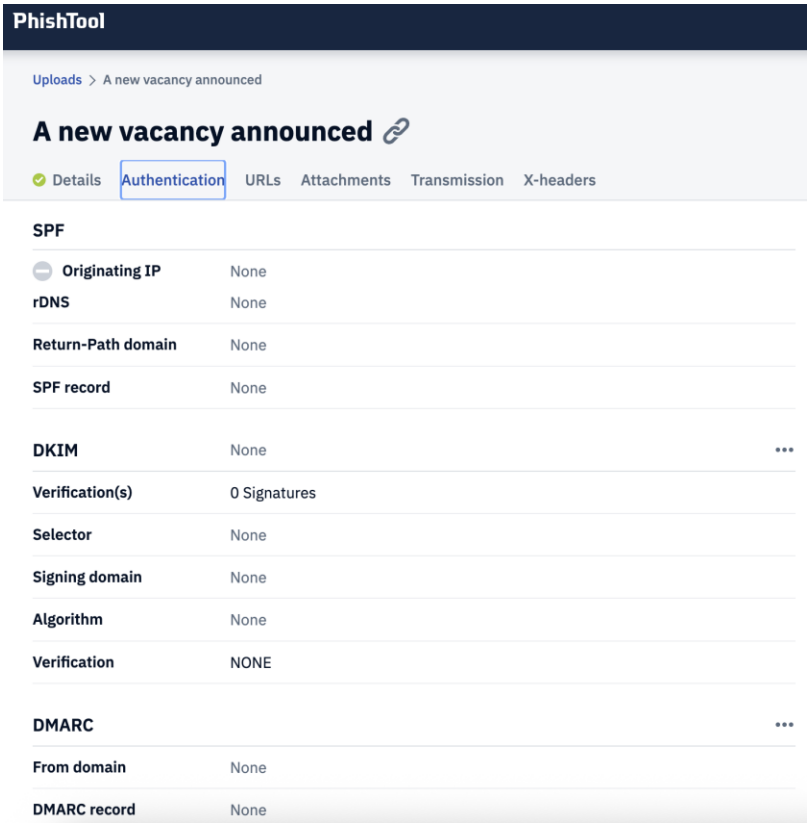


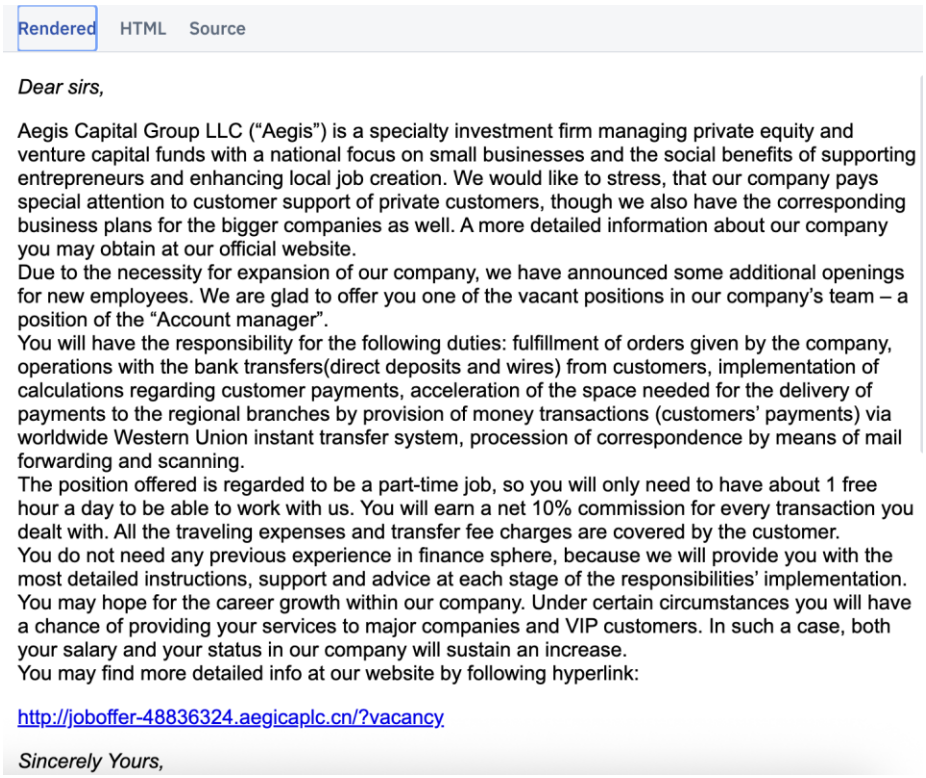
- This email sample was about a Job Offer and was sent out to two employees that worked at the Enron company. A few suspicious things to point out is that there are two from addresses when there should only be one. Furthermore, one of the domain names shows it is from a company "steve.e.ehrenreich@us.arthurandersen.com" and the other sounds like some unknown name "ffbaylis@avto.de". After reviewing the data and reading information about the header and body in the email I moved on to using my tools for analysis. I started with MXToolBox which checks the mail exchange records for a domain and provides details on the mail servers. I entered the first domain name that I found from the email such as "us.arthurandersen.com", and MXLookup results told me no results were found and this is likely because their email servers are decommissioned since the company isn't active anymore. So, then I searched for the other domain which was "avto.de" and MXLookup gave me results on this suspicious domain name. The output gave me an IP address: 109.224.228.62 and next to the IP it says "BUNNYWAY, informacisjke stroitve (AS200325)" Bunnyway is likely the company name. This information tells us where the email came from. Additionally, (AS200325) tells us where the email

actually came from since it is an autonomous system number. (Mx tool Image below)



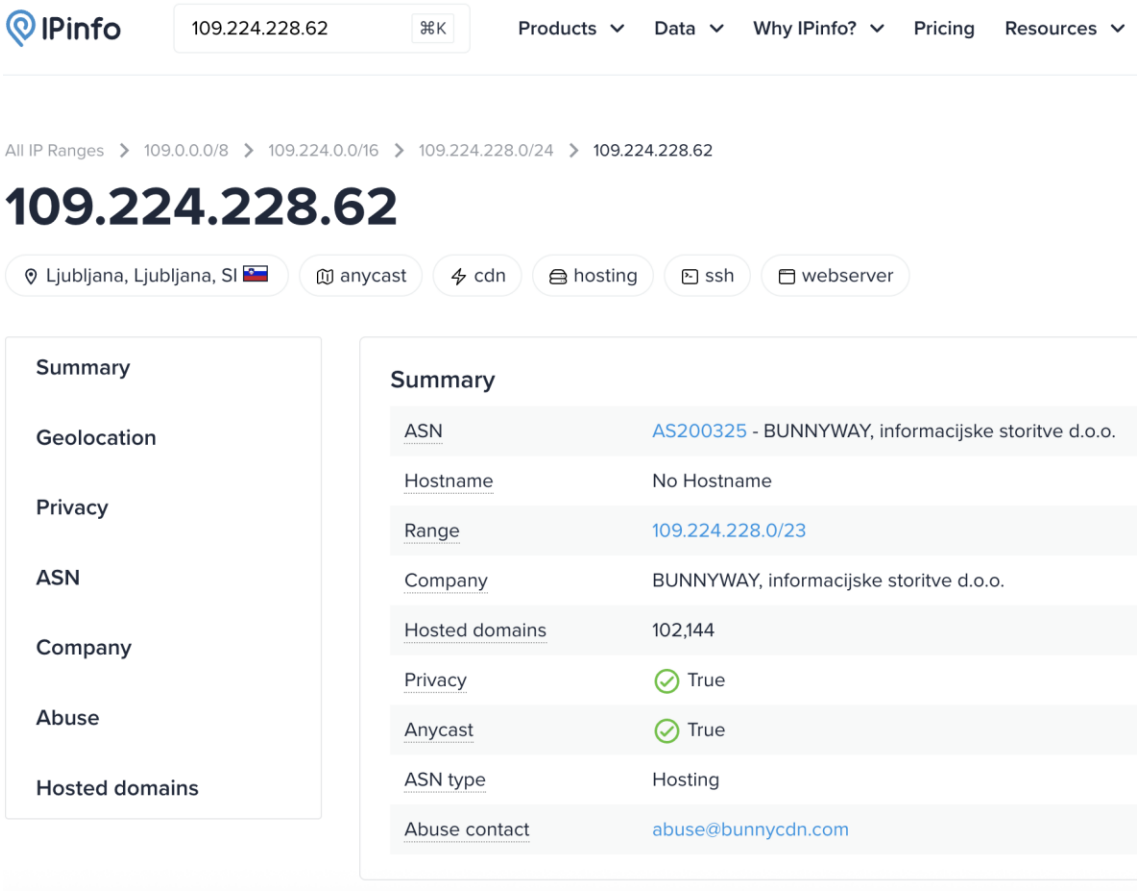
-
- Next, I moved on to PhishTool which is a popular tool to use that deals with detailed detection of phishing emails. Here I uploaded the eml file and it provided me with authentication details. For SPF, DKIM, and DMARC they all stated none which is suspicious, because there is no way to verify the sender. Another important point is that It is possible that an attacker has spoofed the from address and the real one is the second from address which is hidden from the recipient's view. I also found that in the email text the link they used had “http” instead of “https” which majority of legitimate companies use https because it is secure. (images below)



- 

- Next, I used IPinfo.io which allows users to find out more details about the IP address and location. I used the IP address from the suspicious domain "avto.de"

and I found that although the ".de" top-level domain sounds like it should originate from Germany, a Slovenian company server was used as the IP geolocation shows. As we found earlier the server belongs to BUNNYWAY, Informacijske Storitve d.o.o. a legitimate hosting company that manages thousands of domains and websites. This raises suspicion as it seems like there is a mismatch since there is use of a Slovenian server for a German domain.

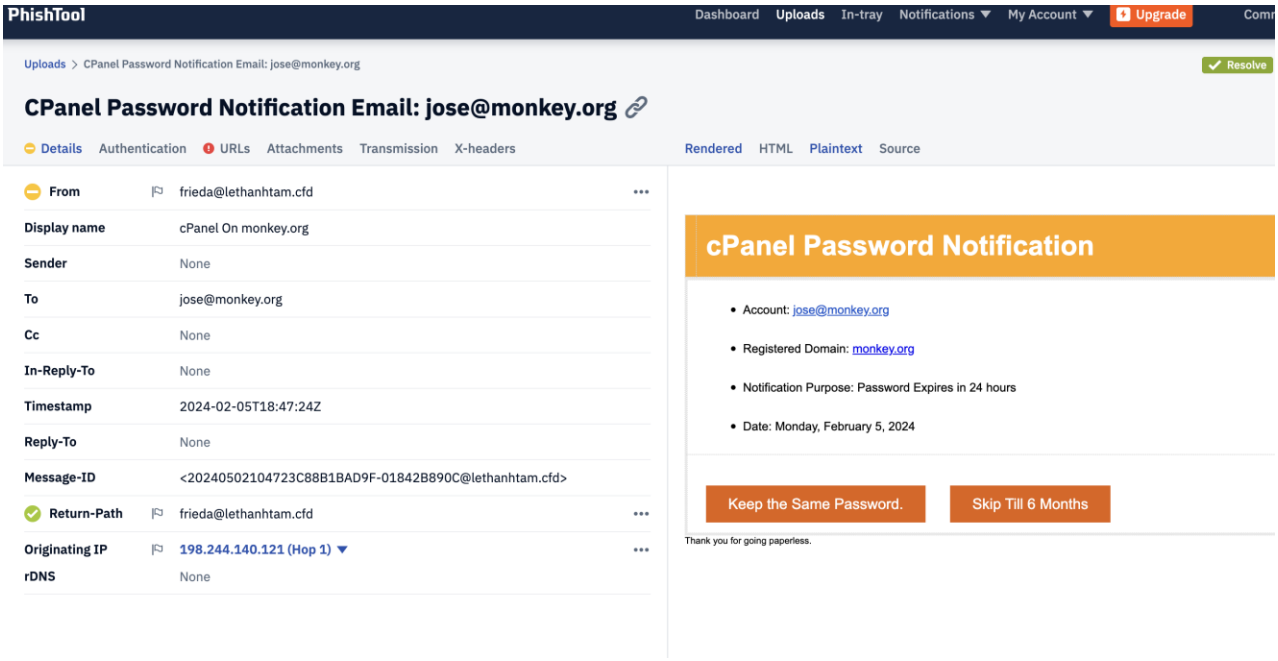


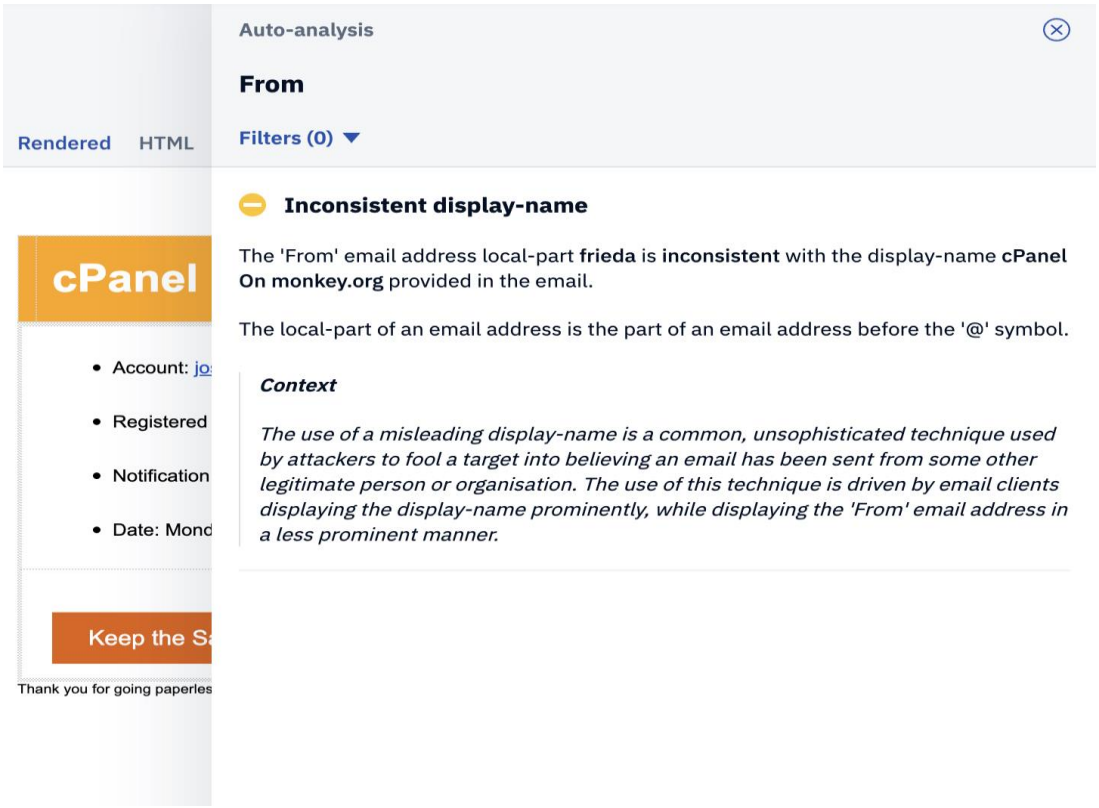
- After performing all the technical analytics, I assessed the **main obvious signs** of phishing just by viewing the email itself. Some of the signs are the two “From’s” in the header address as there should only be one “From”. Adding two of these will trick people and it could also hide the suspicious from address, from being viewed as emails usually show the first from address. Also, the email body states that no previous work experience is needed which is a bit suspicious as most real jobs require previous experience. Another thing is how the sender is randomly messaging them about a job offer but is also offering a high position such as Account Manager. Most phishing scammers will mention high job positions in the message or high salaries to attract individuals to accept their offer.

- My last step is to map this to **MITRE ATT&CK** techniques. The attack used by the attacker was the Spearphishing link attack T1566.002, as they specifically targeted employees from the Enron company while using a spoofed sender address.

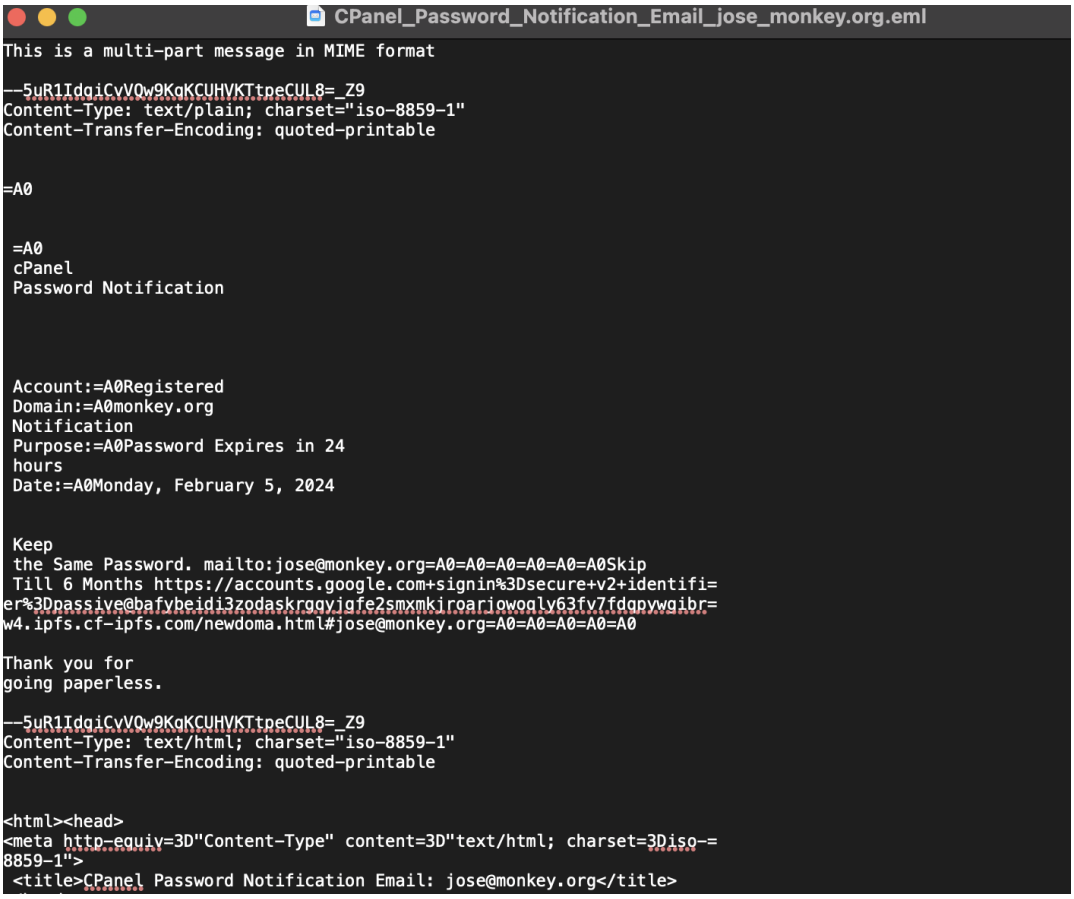
Sample 2 from Nazario: This sample has to do with Password Expiration, and I found the data from Jose Nazario who provides phishing sample data sets on GitHub. The first step is to view the header information and investigate the Return path which is: frieda@lethanhtam.cfd , so we go to MXtoolbox and insert the domain name “lethanhtam.cfd” I found no results at all which could suggest that the attacker wanted to use a domain for temporary use but to further confirm an attacker sent this phishing email I moved on to PhishTool.

- In PhishTool we can see the email format more clearly and it has provided us with important information about the from address such as that attackers usually have an inconsistent from address and display names. They do not match up as the display name says “C Panel on monkey.org” but the from address has to do with .cfd domain name, which is different, so they are implying as if it comes from monkey.org. Most people do not look at the actual sender address anyways, and this is a common technique attackers use.

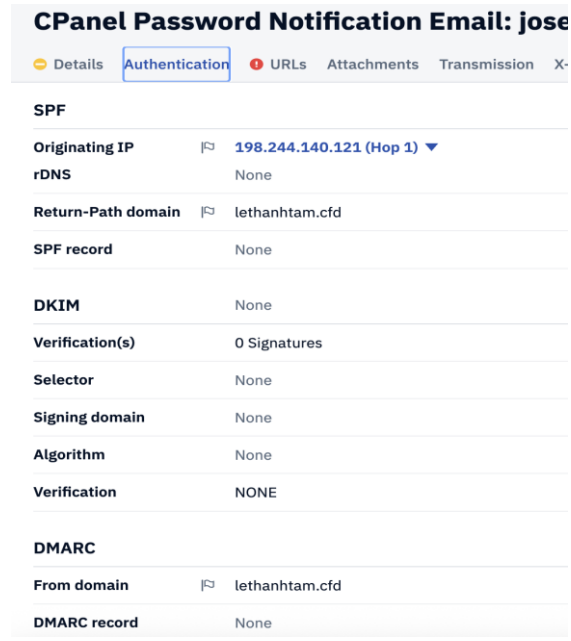


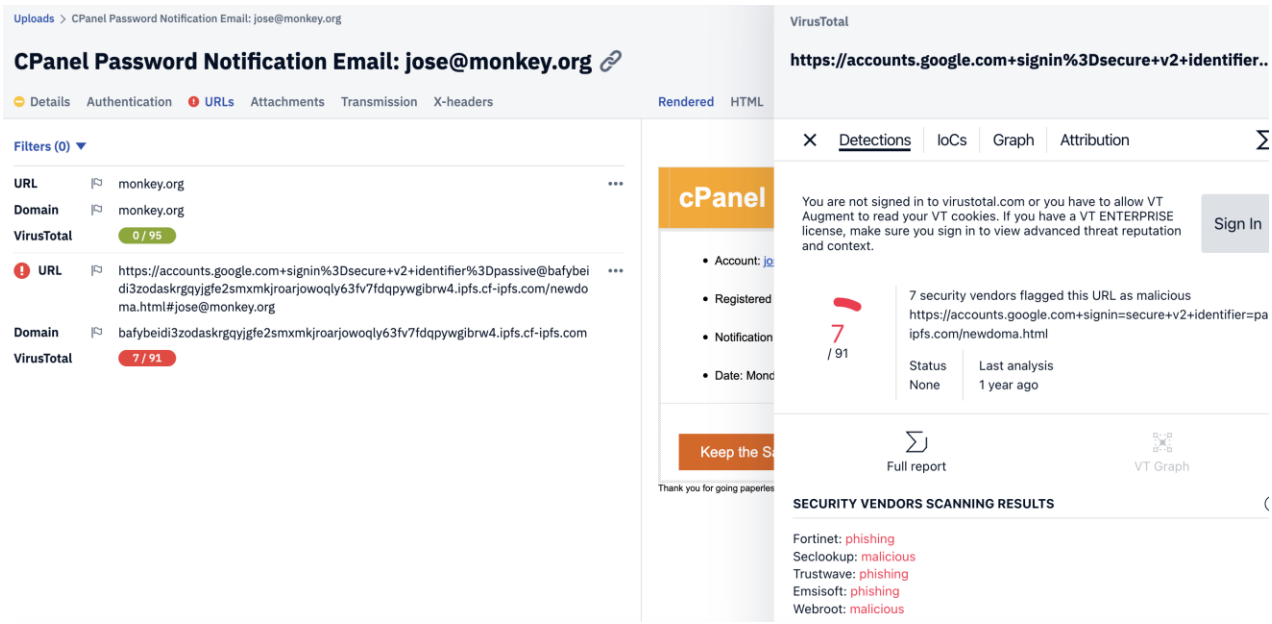


- Phishtool has also provided us with the IP address, which is 198.244.140.121. In PhishTool when hovering over the Keep the same password or Skip till 6 months buttons it will not let you see the full link address. Whereas Text Editor allows you to see the full information and raw data. In Text Editor (view image below) you can see that the links under Keep the same password and Skip till 6 months is a link to google accounts which seems very suspicious because it redirects you to an ipfs page although a legit google account link would be something simpler like this for example: https://accounts.google.com/...etc .

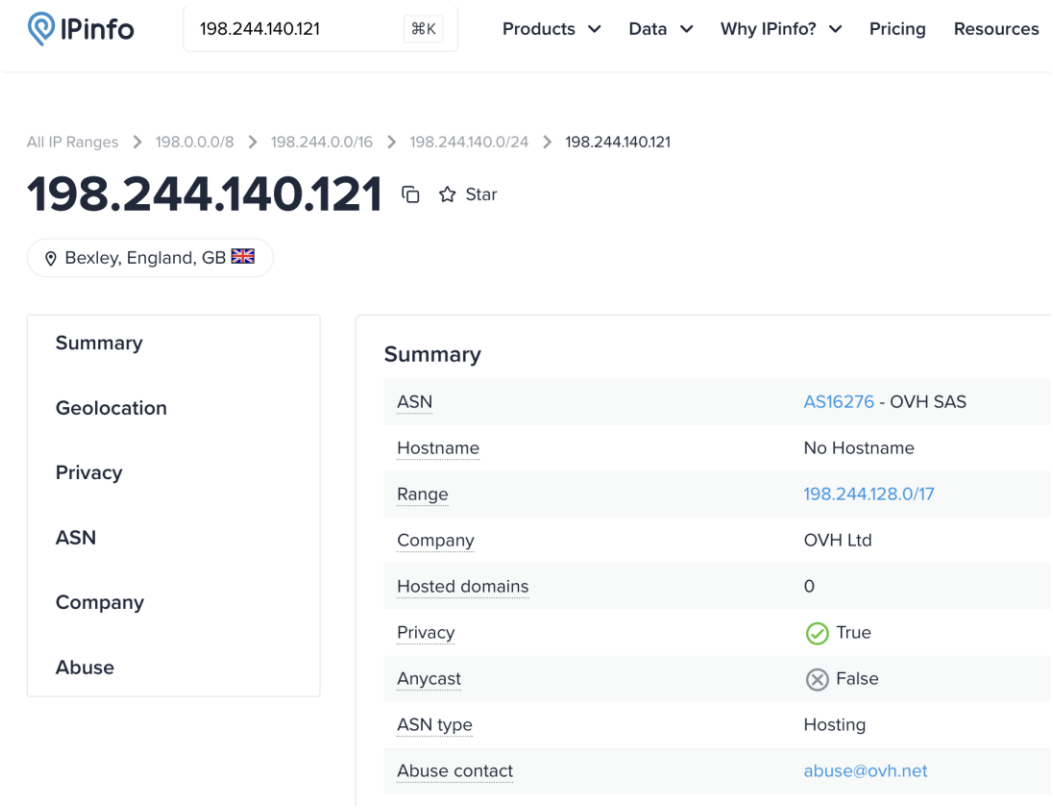


- As shown in the images below, In PhishTool I also found in the authentication section that SPF, DKIM, DMARC all were listed as none and VirusTotal reported 7 security vendors have flagged the same URL as mentioned above, as malicious and phishing which is a red flag.

- 

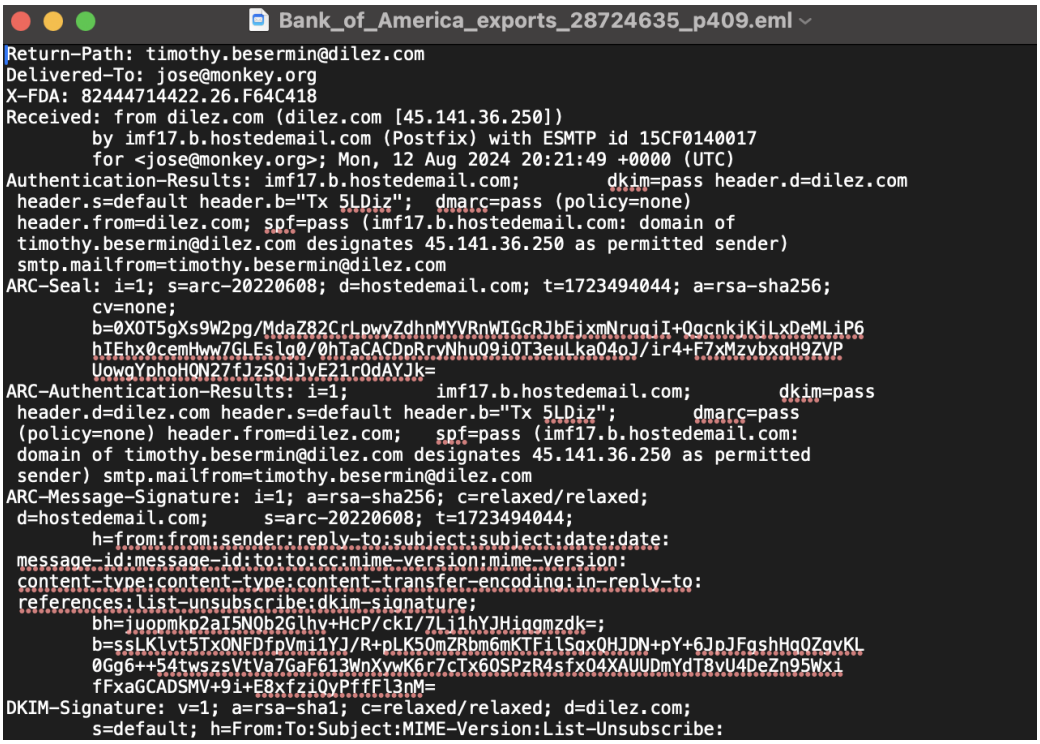


- Moving on to ipinfo.io site, after entering the IP address found for hop 1 which originated this message, it had no hosted domains which is another possible sign the email is coming from an attacker, since they usually use it for temporary purposes like phishing scams. The IP address info also mentions the company was OVH which is a cloud platform, and it is cheap to for hosting domains which may be ideal for scammers since it is easy to use and low cost.

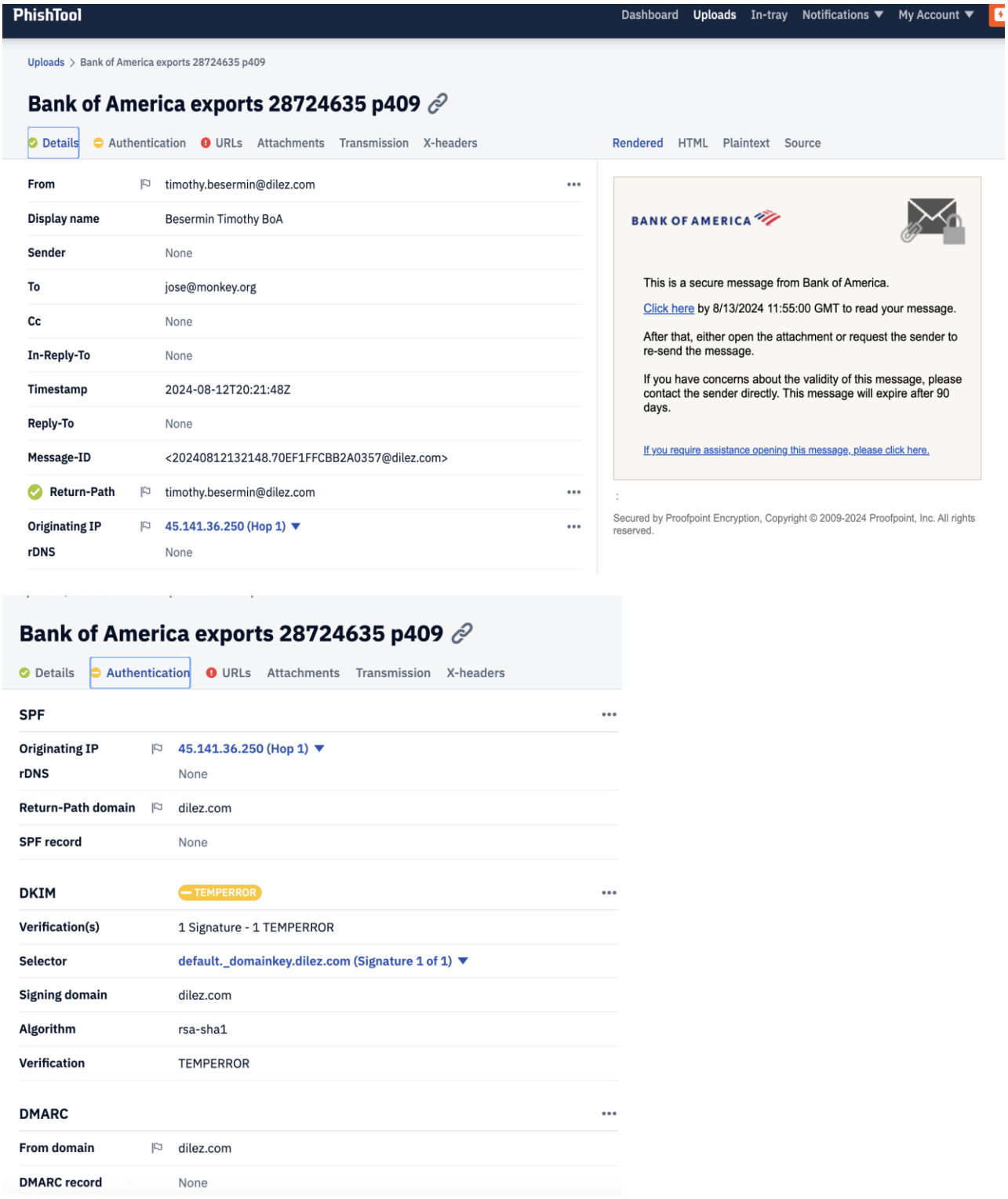


- **Main signs of phishing :** Just by viewing the email in rendered format as it was sent to the recipient, the obvious signs can be the fact that it's a password expiration message as this is a common tactic of scammers, so a person might recognize that as it's very common and they might've probably never received that type of email before. Also, the sender address seems like a random unknown person so that could seem suspicious to others if they take the extra step to view that information. Other than that, I would say this email kind of looks real because of the nice formatting.
- **MITRE ATT&CK:** Phishing T1566 technique was used for this phishing scam since it is general phishing and did not use any links directly and no attachments either.

Sample 3 from Nazario: This sample phishing email is about a Bank of America message. First, I opened the file in Text Editor to view the raw data and looked at the header information that is needed for the analytical process, such as the return path which is: timothy.besermin@dilez.com and the from address dilez.com.

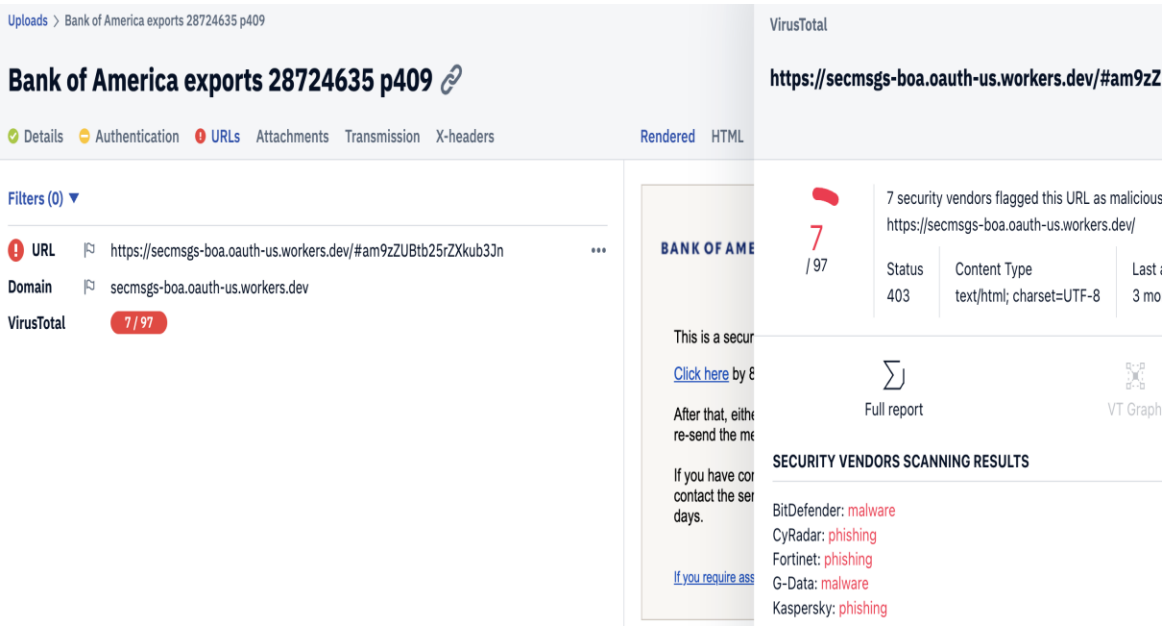


- Moving on, I went on MXToolBox but found no results so then I went to PhishTool to find out more about this email. Some suspicious activity is found as I noticed that the display name is “Besermin Timothy BoA” although the from address has the domain name of “dilez.com” so they are acting as if it comes from Bank of America by including it in the display name, yet the senders address does not have Bank of America in it at all which is a clear sign of phishing. The IP address information is given as 45.141.36.250, and when looking at the authentication section all of them basically say none for SPF, DMARC, and DKIM. This is very suspicious because an official company like Bank of America will always make sure to have everything set up properly. (see image below)

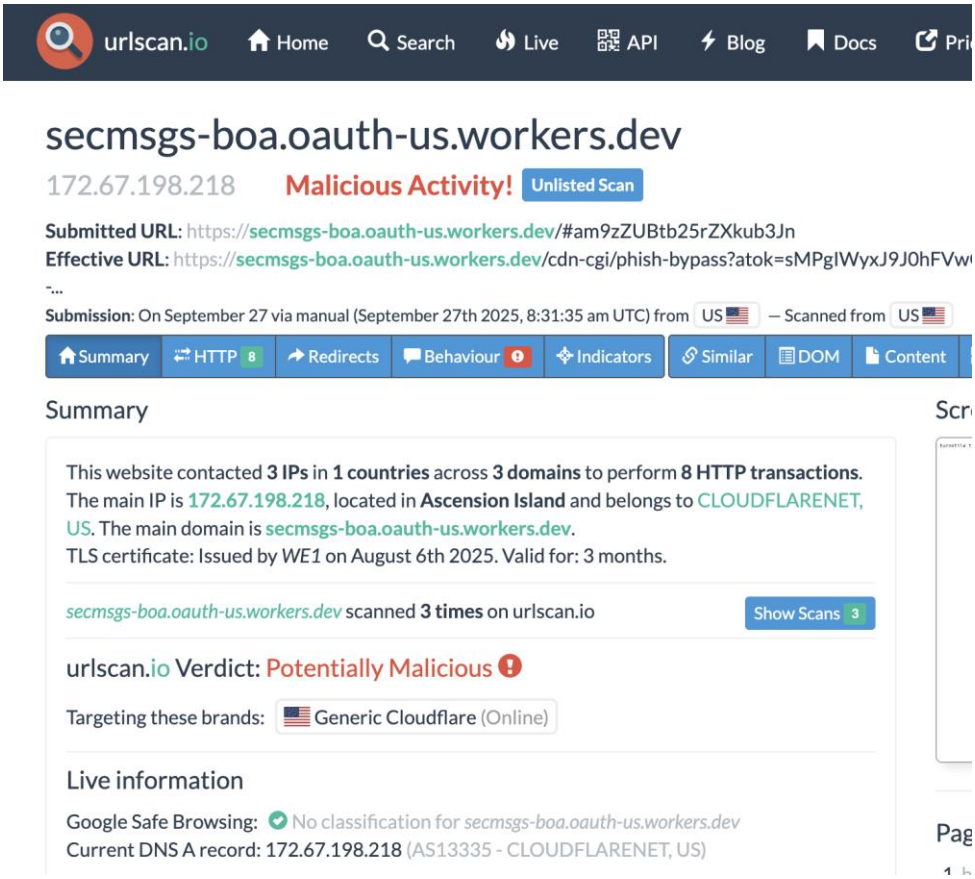


- After going to the URLs section VirusTotal the antivirus detector, has reported that 7 security vendors flagged the URL in the email as malware and phishing. When taking a closer look at the URL “https://secmsgs-boa.oauth-us.workers.dev/#am9zZUBtb25rZXkub3Jn” we can see that in the domain name

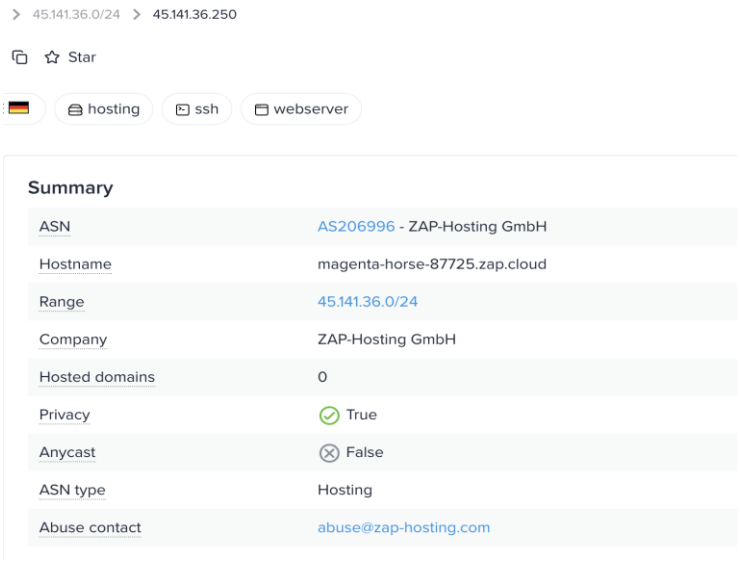
they have included words like “sec msgs” and “boa” which is a phishing technique that is used a lot so when users view links, they will think it is secure.



- Now we will use URLscan.io to see what results we get after performing a URL scan on the URL mentioned above. When entering the URL, we found right away that it gave a warning saying that it is potentially malicious.



- The last tool I used is IPinfo.io and after inputting the ip address we found the location is in Germany. The company is ZAP a hosting server, and this company offers cheap servers, and it is likely for attackers to use this as a source since the cost is low.



- **Main obvious signs**: There is almost a sense of urgency telling the recipient to click on the link by a certain date and warning them that the message will expire in 90 days. If someone were to really look at the email another obvious sign is the dilez.com domain name doesn't make sense. It seems credible at first because the display name says BOA but their email address does not have anything to do with Bank of America.
- **MITRE ATT&CK**: T1566.002 Spearphishing link attack – the attacker adds a malicious link in a phishing email and wants to gain access right away to personal information of the victim.

Security Enhancements & Mitigation Strategies:

- Companies should always require strict SPF, DKIM, and DMARC rules to prevent any phishing attacks which may use methods like spoofing, and enforce secure email gateways with malware detection to check for any suspicious domains.
- Use web content filtering as well to block malicious IPs that are known.

Automation & Advanced Cybersecurity Techniques:

- Detection tools like PhishTool and VirusTotal should be used to check for emails that may be automatically flagged when vendors have found that links are malicious. Perform Investigation to check if links are suspicious or not by using a sandbox or VM.

Awareness & Final Recommendations:

After conducting this analysis and performing phishing threat investigations on these three samples, there are many things to recommend. Many individuals do not consider going the extra mile to check and confirm if the sender can be trusted instead, they will quickly look over the contents of an email message. I recommend that users become more educated and especially in a job setting it should be required and encouraged to train employees on how to analyze an email in at least a short manner. Some simple steps include checking if the display name matches with the sender's address or not. Individuals should also be provided with a "Report Phishing" button so that security teams may take a further look. Other steps are using Multi-Factor Authentication as much as you can, following the principle of Least Privilege Access by only giving employees the amount of access they need, and organizations prioritizing regular updates on mail servers to reduce any chances of risk. In the real-world phishing scams

occur often like in platforms such as LinkedIn where job offers are being posted about, popular companies like Google are also being impersonated to trick victims into giving up credentials, and more. The samples I have analyzed above happen often in the real world and many fall for the scams. Overall, after my research and investigation I have a better understanding of how advanced these phishing scams are becoming and that we must take it more seriously to focus on security awareness and implementing best practices when it comes to protecting ourselves and our data.

References

Cloudfare. What are DMARC, DKIM, and SPF? https://www.cloudflare.com/learning/email-security/dmarc-dkim-spf/

Diego, C. *Diegoocampoh/machinelearningphishing: This project will determinewhich of the five supervised classification machine learning algorithms performs best in detecting Phishy emails*. GitHub. https://github.com/diegoocampoh/MachineLearningPhishing

Shanice. (2025, July 2). *Complete guide to phishing: Techniques & mitigations*. Valimail. https://www.valimail.com/resources/guides/guide-to-phishing/

Sunknighteric. (2023). *Sunknighteric/EPVME-dataset: A new malicious email dataset*. GitHub. https://github.com/sunknighteric/EPVME-Dataset/