

Email Header Analysis

By:

Oladayo Akinyode

Supervisor: Mr. Olaitan

Overview

The email was delivered to Olaitan Oladapo on 15th August 2024 with timestamp 08:37:08 – 0700(PDT). The email was moved to spam by Olaitan's email domain which is Hotmail. The suspected attacker was acting all friendly with a threat tone to leak private videos and pictures, He/she was talking about how Olaitan has been using social media and some sketchy sites, the attacker was describing how he/she has been extracting Olaitan information from the sites and promised to release the video to all the contact if the user fail to make payment of bitcoin equivalent to \$1000 in bitcoin to the following bitcoin address: 1ZrNNiff9LVEh1EXmTiHazzmW1vSAhtp.

The sender's name is Sipes Phoebe with the email address: resqurobactndes@hotmail.com

Method/ Approach

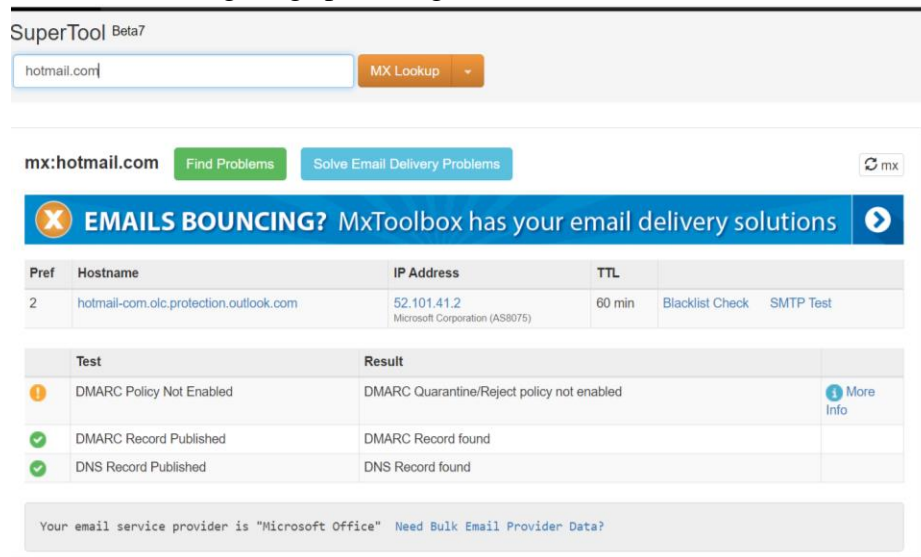
The email analysis started by analyzing the content of the message, The email consist of some phishing indicators:

- Threat Language
- Sense of Urgency
- Tone of the message
- Inclusion of phishing link

Analysis

I analyze the email and the IP address using three different tools Mx toolbox, Epieos, and abuse ipdb. This is the result generated from the using the email and IP address.

Mx toolbox: I looked up the email address and saw that the email has been blacklisted by different users sighting spamming



SuperTool Beta7

hotmail.com MX Lookup

mx:hotmail.com Find Problems Solve Email Delivery Problems

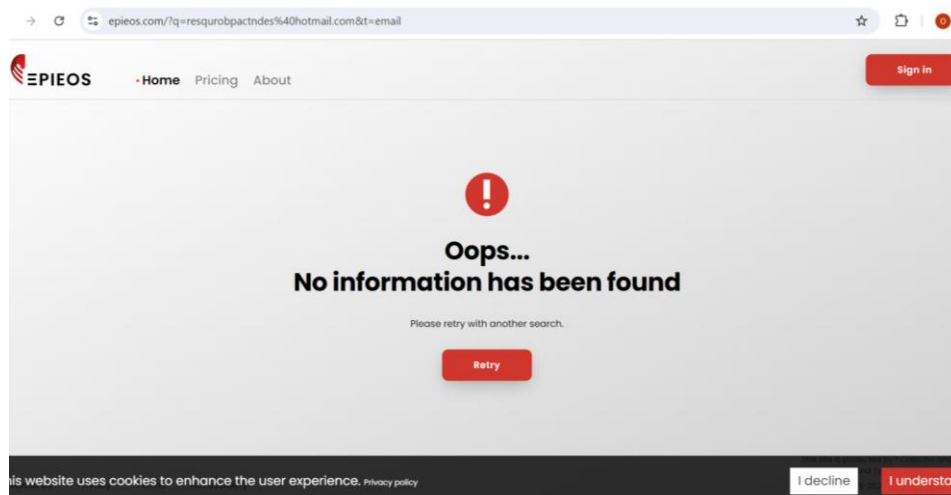
EMAILS BOUNCING? MxToolbox has your email delivery solutions

Pref	Hostname	IP Address	TTL	
2	hotmail-com.olc.protection.outlook.com	52.101.41.2 Microsoft Corporation (AS8075)	60 min	Blacklist Check SMTP Test

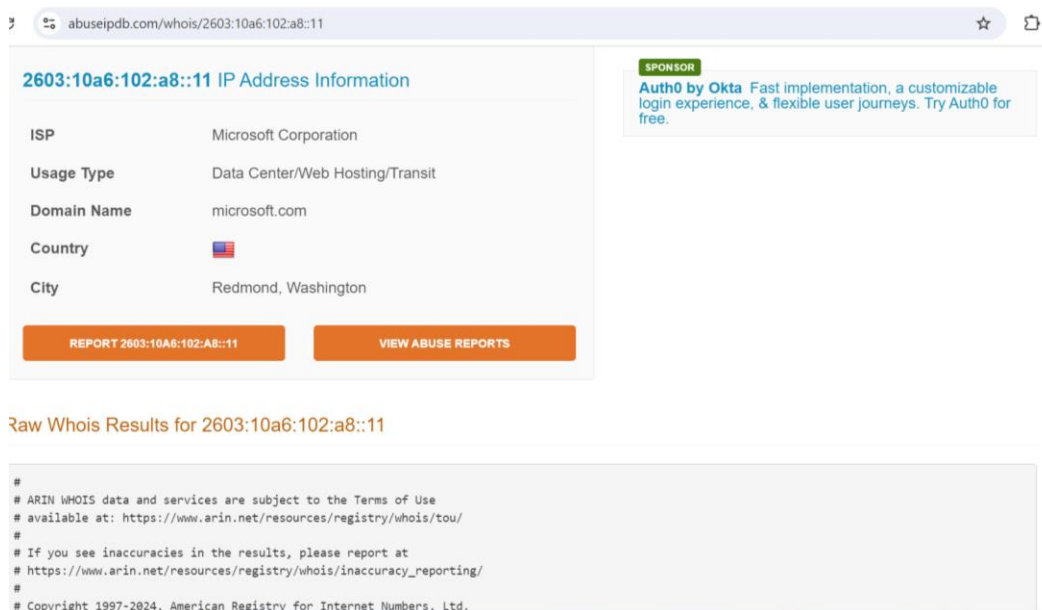
Test	Result	
DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info
DMARC Record Published	DMARC Record found	
DNS Record Published	DNS Record found	

Your email service provider is "Microsoft Office" [Need Bulk Email Provider Data?](#)

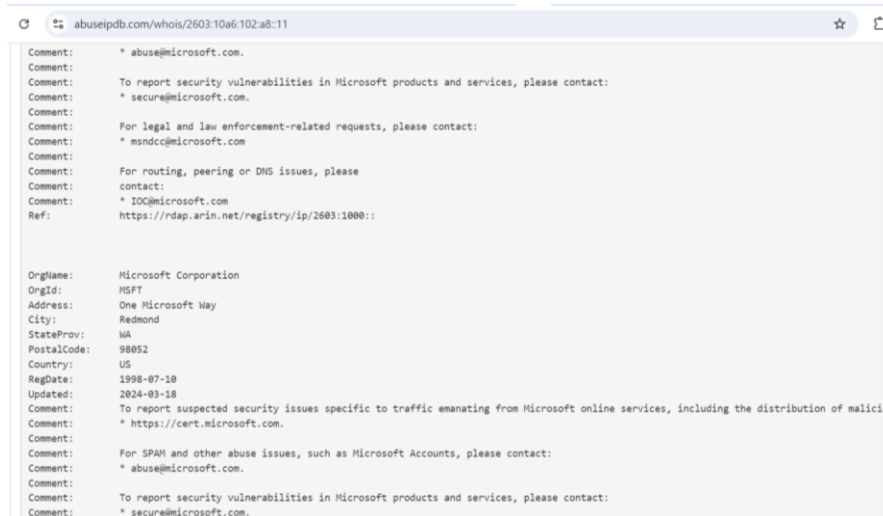
Epieos: The tool does not have any information regarding the email in their database.



Abuse Ipdb: This tool has some information about the location of the attacker in their database. I used the IP address. The tool showed us that the attacker is located at Redmond Washington in the U.S.



The second image below shows further information about the IP address: **2603:10a6:102:a8::11**



The three tools we used established that the owner of the email and the IP address has been reported as spam, abuse, and malicious.

Impression of the sender

The impression of the sender is malicious and the sender aims to defraud the owner of the email through the bitcoin address: 1ZrNNiff9LVEh1EXmTiHazzmW1vSAhtp.

Conclusion

The IP address and email address belong to a malicious user in the U.S.A. where the receiver of this email does not have any relatives, furthermore, the tone of the email shows threat, urgency, bitcoin address to defraud the user of \$1000 and my analysis using three different tools shows that the user is malicious and the intention is to defraud the email user. Additionally, the attacker is just learning the trade because of the content, and the tone of the message.

Recommendations

This is my recommendation:

- The receiver should report the email for phishing and block the email.
- The user should not make payment to the address and should always report this kind of email to the SOC team or government agencies.
- If this email is received by a couple of our staff, our team should organize end-user training to sensitize the staff more about this kind of malicious email.