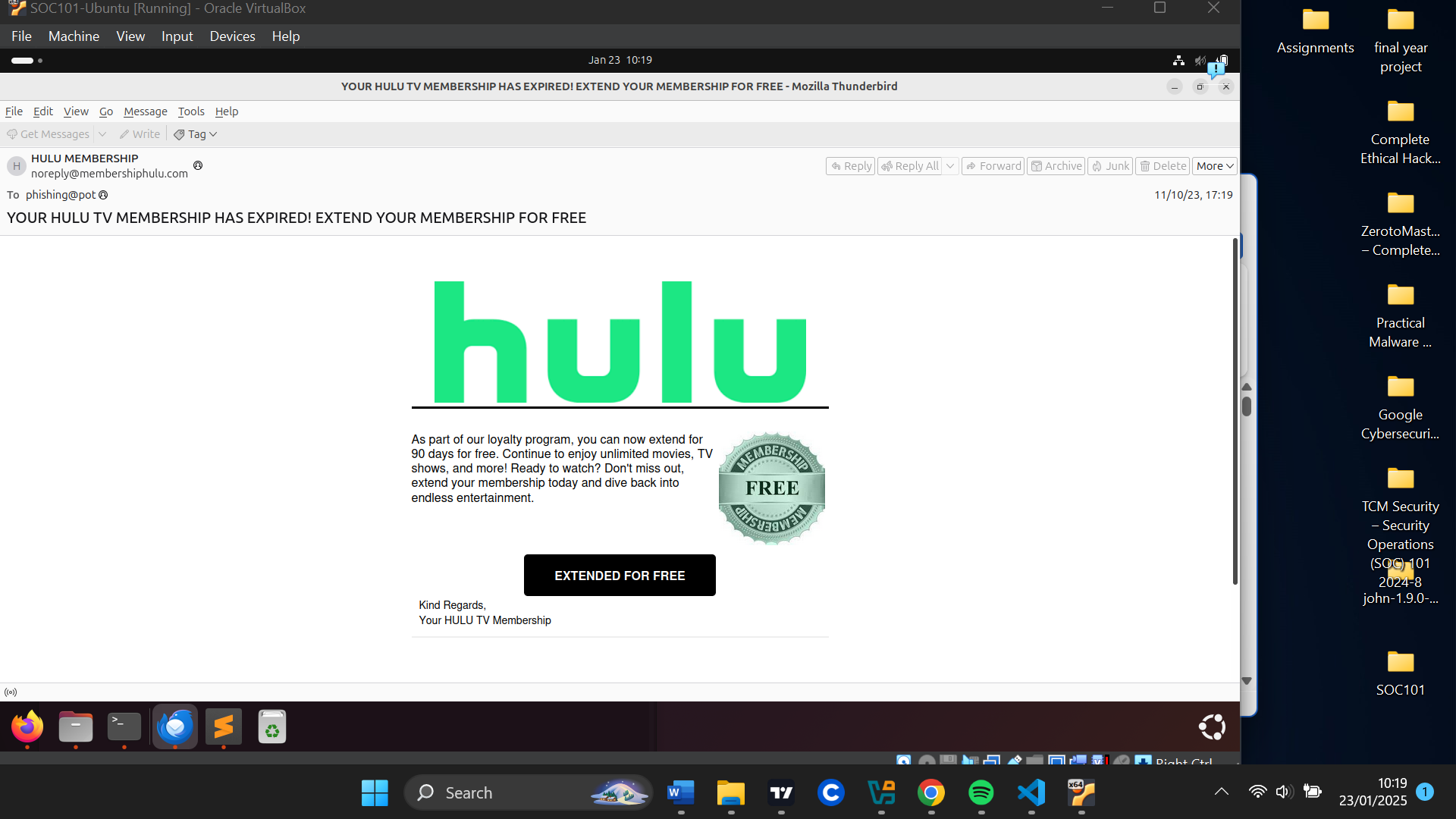
Sample-1899. eml



HEADERS:

**Date/ Time**: 05:19 pm, Nov 10th 2023

**Subject**: YOUR HULU TV MEMBERSHIP HAS EXPIRED! EXTEND YOUR MEMBERSHIP FOR FREE

**To**: phishing@pot

**From**: noreply@membershiphulu.com

**Reply to**: -

**Return-Path**: bounce@bigsbie.com

**Sender IP**: 89.144.12.8

**Resolved host**:

**Message – ID:** aa16a90f-287f-490b-85fc-3313a29864cf@DM6NAM12FT025.eop-nam12.prod.protection.outlook.com

URLs

“hxxps[://]t[.]co/8ItGjWbzhy”

"hxxps[://]t[.]co/dJ6gFSwFJF”

ATTACHMENT:

-

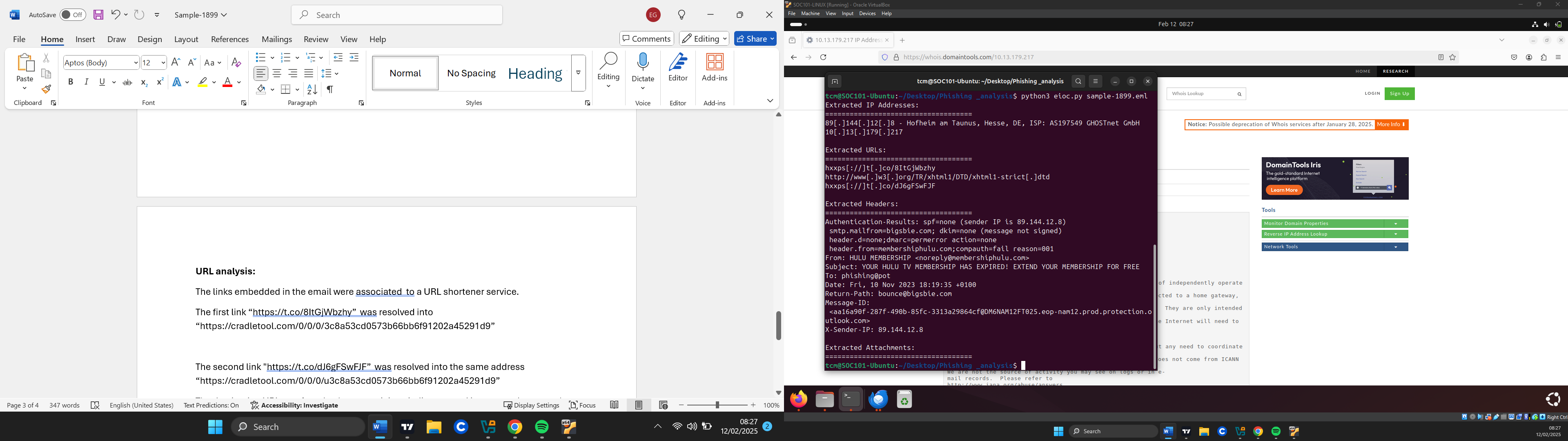
E-MAIL DESCRIPTION

The email appears to be coming from hulu, which is a streaming media service.

It is notifying the user to extend their membership for free as part of some loyalty program since their membership has expired.

There is a call-to-action button “extend for free” where the user is supposed to click to extend their membership for free for 90 days. The whole email body, however, is clickable.

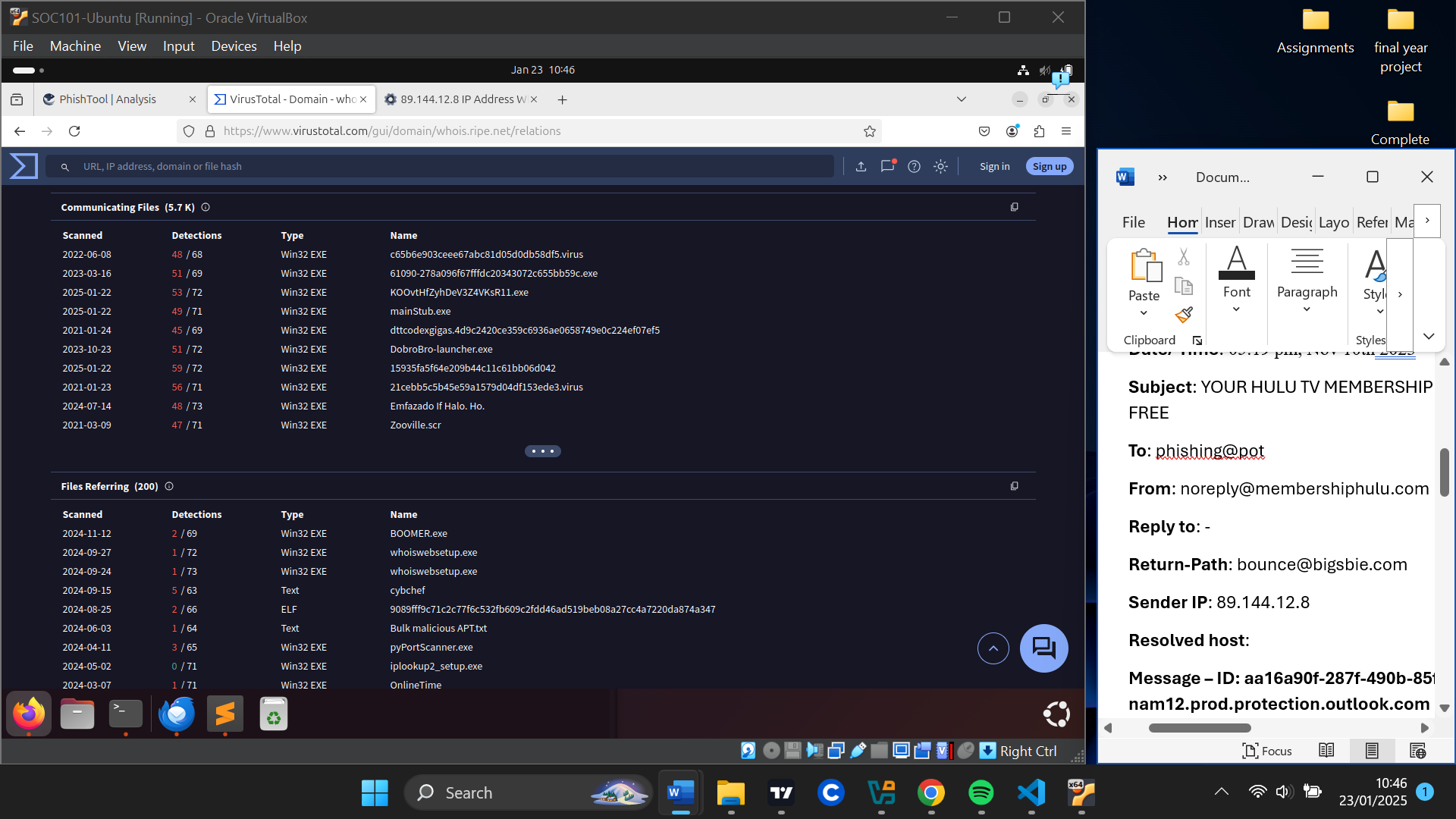
Our python script was used to extract all information about the email and indicated the email contains some URLs.



ARTIFACT ANALYSIS:

**Sender analysis:**

The senders’ Ip address does not resolve any host however the server associated with the Ip address is suspicious because it has a lot of relations with malicious files as well as communicates with a lot of malicious files.



The domain related to the sender “membershiphulu.com” has been flagged as malicious making this email suspicious.

A screenshot of a computer

Description automatically generated

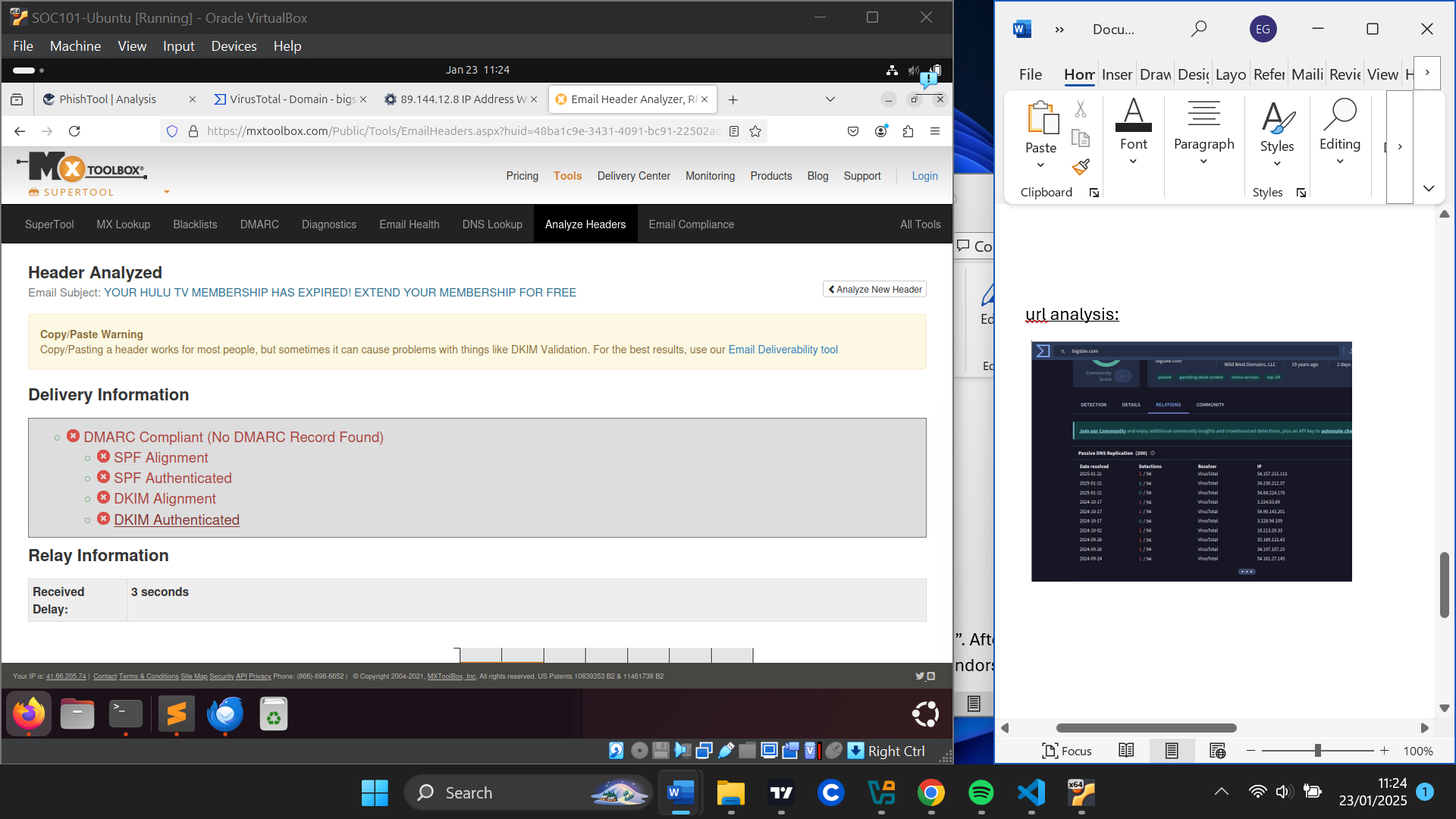
The return-path domain “bigsbie[.]com” is inconsistent with the from domain “membershiphulu[.]com”.

“bigsbie[.]com” although being a legitimate domain has been seen to make DNS resolutions to suspicious addresses.

A screenshot of a computer

Description automatically generated

The email header failed all email authentication methods indicating possible spoofing and this makes the email very suspicious.



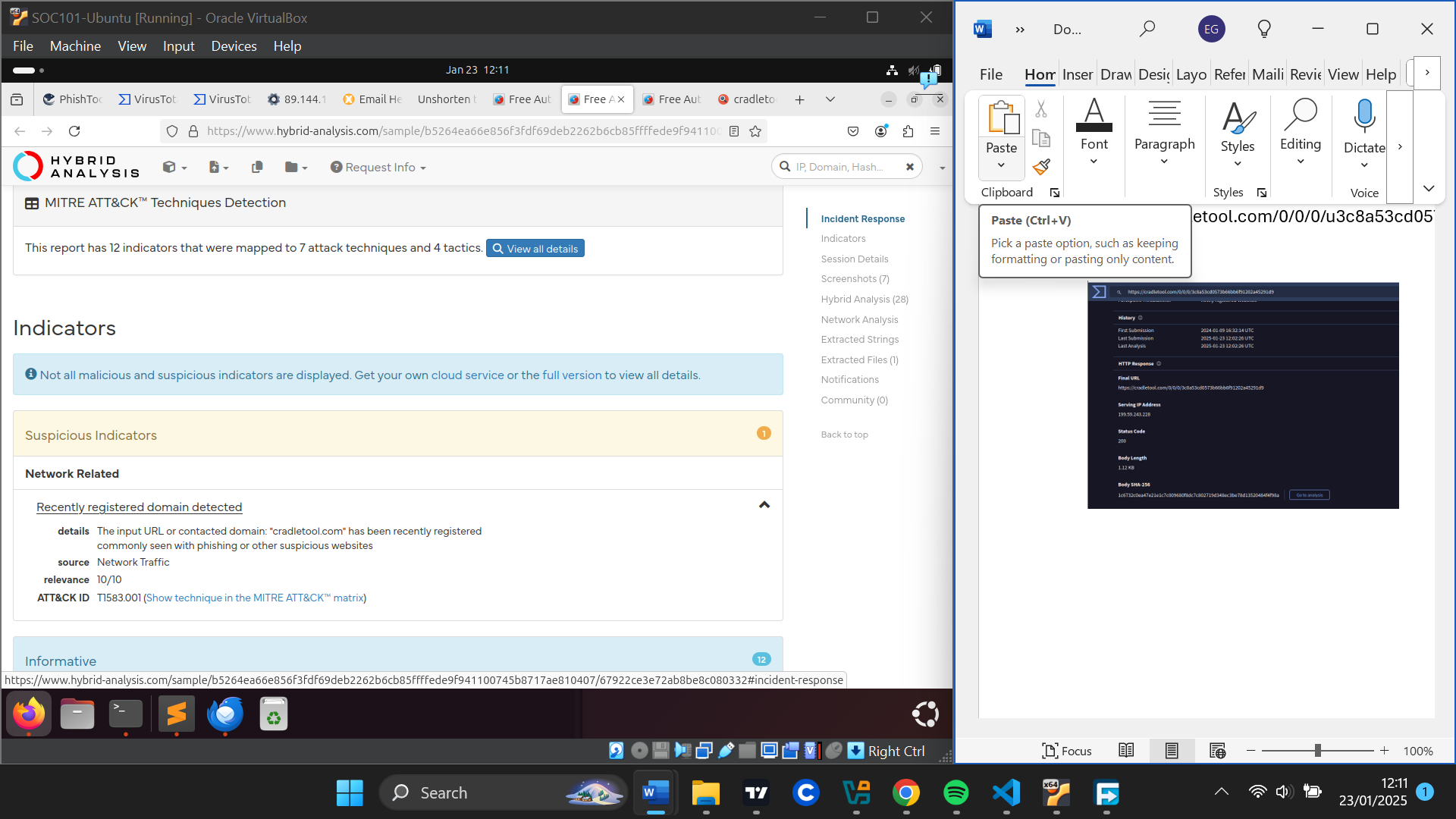
**URL analysis:**

The links embedded in the email were associated with a URL shortener service.

The first link“hxxps[://]t[.]co/8ItGjWbzhy” was resolved into “hxxps[://]cradletool[.]com/0/0/0/3c8a53cd0573b66bb6f91202a45291d9”

The second link "hxxps[://]t[.]co/dJ6gFSwFJF” was resolved into the same address “hxxps[://]cradletool[.]com/0/0/0/3c8a53cd0573b66bb6f91202a45291d9”

The destination URL was found to have suspicious indicators and is commonly seen to be linked with phishing and other suspicious websites and was also recently registered according to hybrid analysis.



**Attachment analysis:**

**-**

VERDICT

Due to the senders’ Ip address being related to malicious files and failing email authentication methods and also the sender’s domain being flagged malicious, it is safe to say this a phishing email.

Additionally, the URLs embedded were found to lead to a suspicious website found to have suspicious indicators linked with phishing.

DEFENSE ACTIONS

To ensure users never visit the malicious website, I have blocked the URL “hxxps[://]cradletool[.]com/0/0/0/3c8a53cd0573b66bb6f91202a45291d9”

I have also blocked any request to or from the domain “membershiphulu.com”

And lastly, I have blocked any emails coming from “noreply@membershiphulu.com”