Sample-1643

A screenshot of a computer

AI-generated content may be incorrect.

HEADERS:

**Date/ Time**: 07:49 pm, Oct 22nd 2023

**Subject: AAVE: ($AAVE) Airdrop Claim**

**To**: phishing@pot

**From**: noreply@messages.homeaway.com

**Reply to**: -

**Return-Path**: noreply@messages.homeaway.com

|  |  |
| --- | --- |
|  |  |

**Sender IP**: 140.238.151.68

**Resolved host**: webmail2.mts.syn-alias.com

**Message – ID:** <621f71f2c9001186a3a39314a45a11e6@localhost>

URLs

When I run our eioc.py script on the email we retrieved some urls :

hxxps[://]aave[.]com/claim[.]

hxxps[://]aave[.]com/claim

hxxps[://]app[.]aave[.]com/

hxxps[://]mandrillapp[.]com/track/click/30255250/www[.]giorgiobarbagelata[.]eu?p=eyJzIjoiOGZTS3BlTWlSTGNsMkNFVFVVOHVCN3JYQXNFIiwidiI6MSwicCI6IntcInVcIjozMDI1NTI1MCxcInZcIjoxLFwidXJsXCI6XCJodHRwczpcXFwvXFxcL3d3dy5naW9yZ2lvYmFyYmFnZWxhdGEuZXVcXFwvQ29hdGluZy5odG1sXCIsXCJpZFwiOlwiNmJhYTllMTA2Y2U1NGI0NzkyMTZjNzg0NWRlYTRkNTBcIixcInVybF9pZHNcIjpbXCI4Y2IyOWQ2MTkyMTAyYWZkZGIxZTM3MGE1MTk2Njk0MjRmMzhiNDRkXCJdfSJ9

ATTACHMENT:

E-MAIL DESCRIPTION

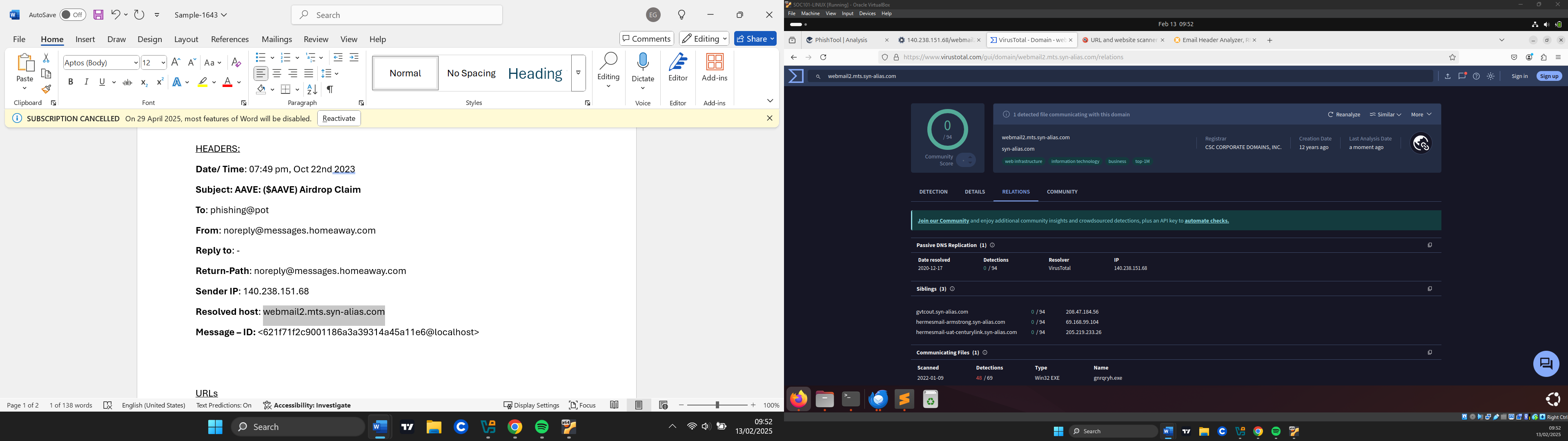
The email appears to be from aave , a cryptocurrency liquidity protocol , regarding an airdrop claim . It states that the recipient is eligible for an aidrop of the AAVE tokens and to claim the airdrop, he has to visit a link “ hxxps[://]aave[.]com/claim”.

There Is some sort of urgency here stating the airdrop claim validity lasts until 25th October 2023. Which Is three days after the email was sent.

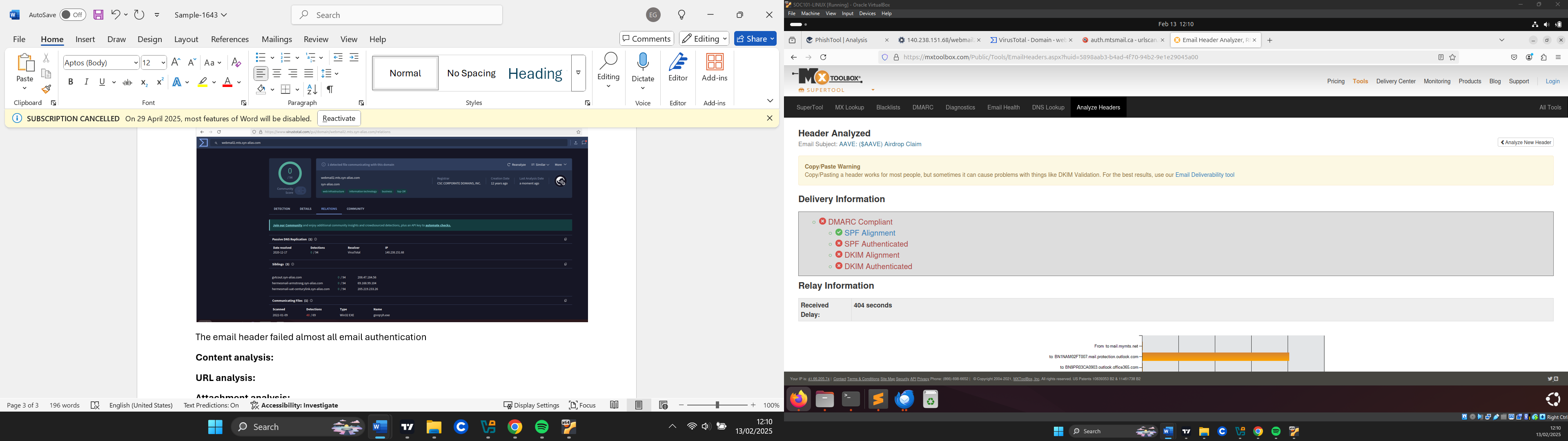
ARTIFACT ANALYSIS:

**Sender analysis:**

When the reputation of the host related to the senders IP address (“ webmail2[.]mts[.]syn-alias[.]com”) was checked it appeared to look clean. But the resolved host had one file communicating with the domain and this communicating file was found to be malicious by lots of vendors. This makes the host suspicious.



The email header failed almost all email authentication methods indicating it is possibly spoofed.



The sender’s email domain (“homeaway.com”) appeared clean on multiple sources but has had communication with malicious files and has malicious files that contain the domain. This makes the domain highly suspicious.

A screenshot of a computer

AI-generated content may be incorrect.

**URL analysis:**

All links related to the AAVE website ( hxxps[://]aave[.]com/claim , hxxps[://]app[.]aave[.]com/) appeared to be legitimate and clean however , when you hover over any of these links in the email it appears to have the same URL as the other URL extracted.

The second URL (“hxxps[://]mandrillapp[.]com/track/click/30255250/www[.]giorgiobarbagelata[.]eu?p=eyJzIjoiOGZTS3BlTWlSTGNsMkNFVFVVOHVCN3JYQXNFIiwidiI6MSwicCI6IntcInVcIjozMDI1NTI1MCxcInZcIjoxLFwidXJsXCI6XCJodHRwczpcXFwvXFxcL3d3dy5naW9yZ2lvYmFyYmFnZWxhdGEuZXVcXFwvQ29hdGluZy5odG1sXCIsXCJpZFwiOlwiNmJhYTllMTA2Y2U1NGI0NzkyMTZjNzg0NWRlYTRkNTBcIixcInVybF9pZHNcIjpbXCI4Y2IyOWQ2MTkyMTAyYWZkZGIxZTM3MGE1MTk2Njk0MjRmMzhiNDRkXCJdfSJ9”) appears to be malicious and linked with “Phishing”.

A screenshot of a computer

AI-generated content may be incorrect.

This shows the URL names related to AAVE that appear in the email body have been used to mask the malicious phishing link.

**Attachment analysis:**

**-**

VERDICT

Due to the host of the senders IP address being suspicious and also the email reputation being spoofed.

Also, the destination of all URLs in the email point to a malicious URLs which is malicious (tagged as phishing).

It is safe to say that this email is a phishing email

DEFENSE ACTIONS

To prevent users from visiting the malicious website, I have blocked access to the URL (“hxxps[://]mandrillapp[.]com/track/click/30255250/www[.]giorgiobarbagelata[.]eu?p=eyJzIjoiOGZTS3BlTWlSTGNsMkNFVFVVOHVCN3JYQXNFIiwidiI6MSwicCI6IntcInVcIjozMDI1NTI1MCxcInZcIjoxLFwidXJsXCI6XCJodHRwczpcXFwvXFxcL3d3dy5naW9yZ2lvYmFyYmFnZWxhdGEuZXVcXFwvQ29hdGluZy5odG1sXCIsXCJpZFwiOlwiNmJhYTllMTA2Y2U1NGI0NzkyMTZjNzg0NWRlYTRkNTBcIixcInVybF9pZHNcIjpbXCI4Y2IyOWQ2MTkyMTAyYWZkZGIxZTM3MGE1MTk2Njk0MjRmMzhiNDRkXCJdfSJ9”)