

Shown above is the generated alert via **LetsDefend** with the provided alert information.

Objective 1: When was the alert sent ?

A screenshot of a computer

Description automatically generated

After opening email security while filtering to Trentons email, it shows that the email was sent June 13th, 2021, at 02:11 hours. Not only I know the exact time the email was sent but I am able to discover that there is also a document attached to the email.

Objective 2: What is the email's SMTP address?

(Continued next page)

A screenshot of a computer

Description automatically generated

According to the alert information provided, the SMTP also known as the Simple Mail Transfer Protocol address is 24.213.228.54.

Objective 3: What is the sender address?

A screenshot of a computer

Description automatically generated

As shown in the above image, the senders address is [trenton@tritowncomputers.com](mailto:trenton@tritowncomputers.com).

Objective 4: What is the recipient address?

(Continued next page)

A screenshot of a computer

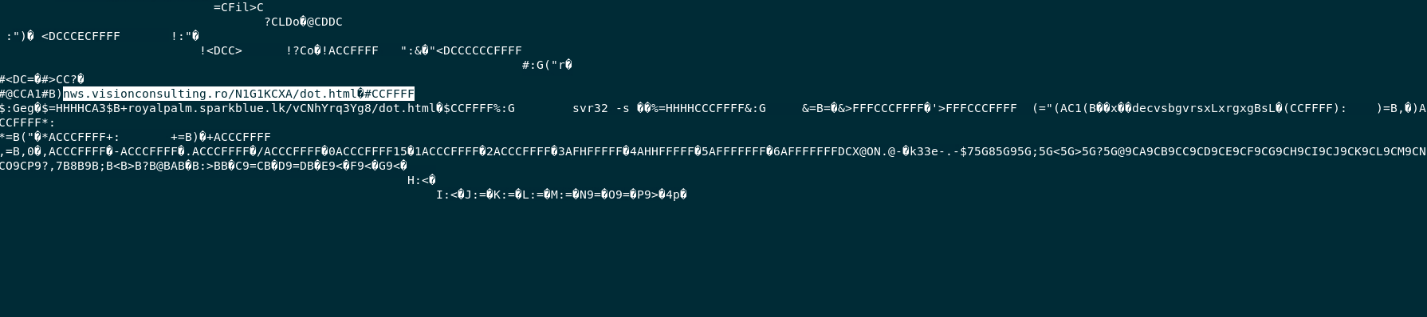
Description automatically generated

As shown in the image above, the recipients address is [lars@letsdefend.io](mailto:lars@letsdefend.io).

Objective 5: Is the mail content suspicious?A screenshot of a computer

Description automatically generated

I have used the Linux Sandbox distributed by **LetsDefend** to download and extract the zipped file (**unzip [filename]**) using the command line. Based on my analysis, I have determined these two files could possibly be suspicious. But as any analyst should... let’s dig a little deeper.



Investigating further in the file I see there is a URL link of nws.visionconsulting.ro/N1G1KCXA/dot.HTML

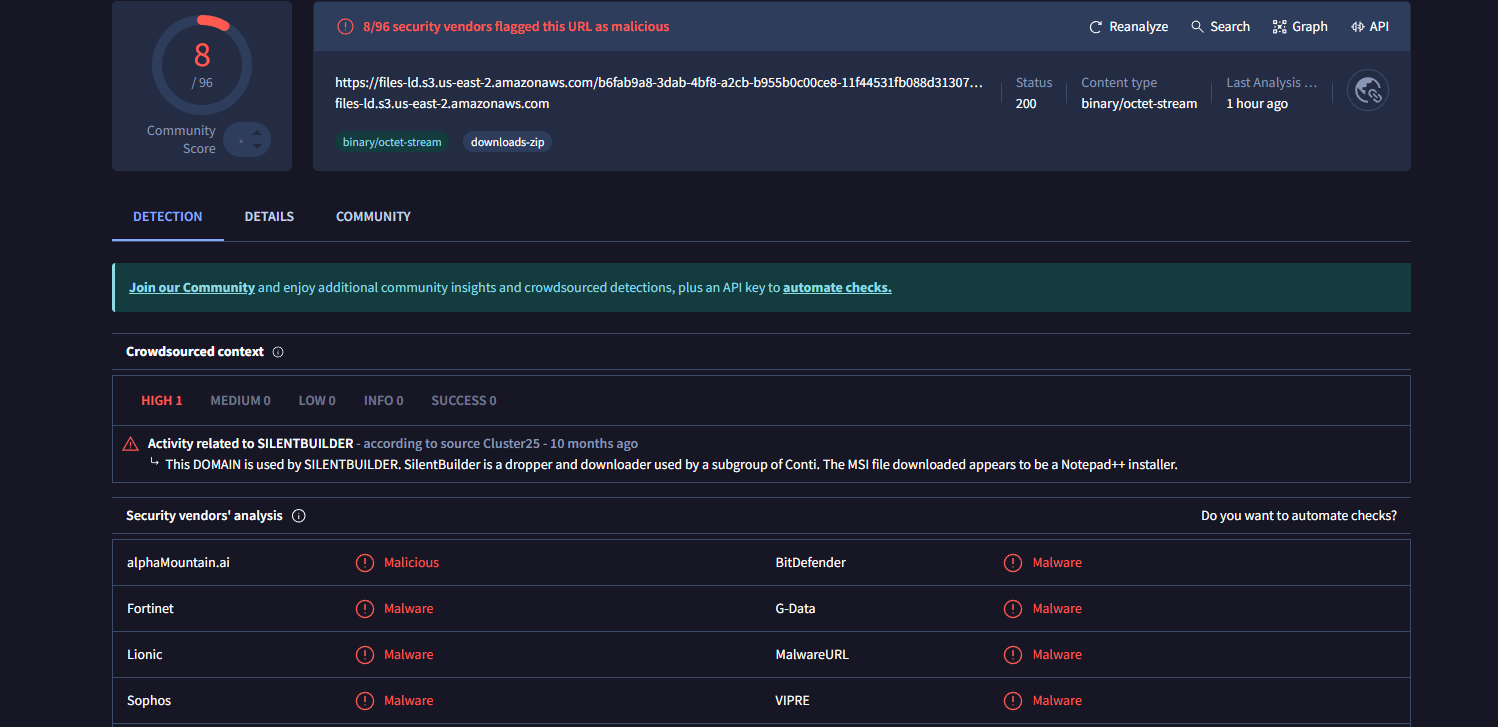
Objective 6: Is there any attachment?

(Continued Below)

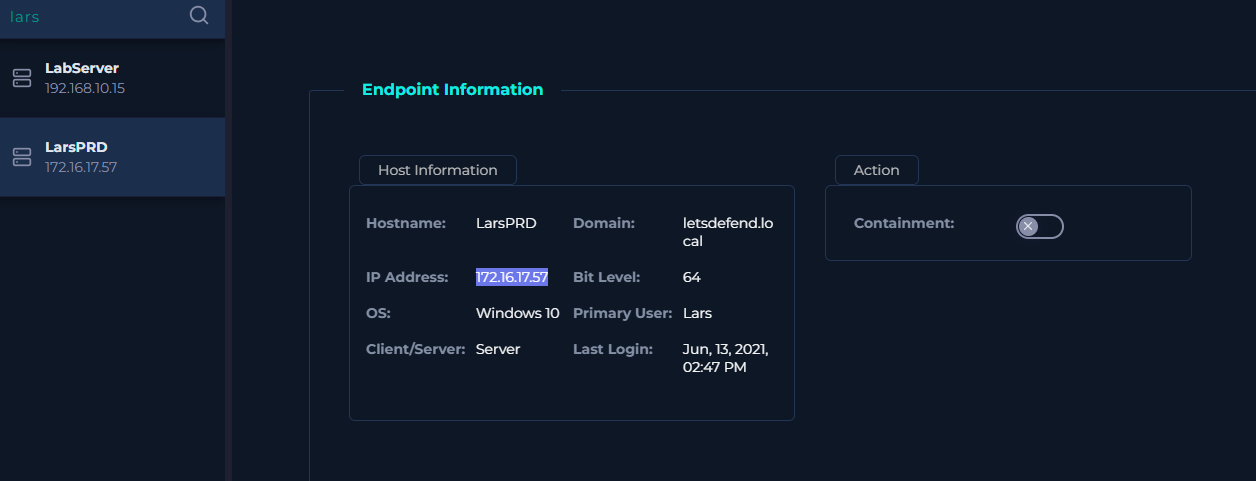
A screenshot of a computer

Description automatically generated

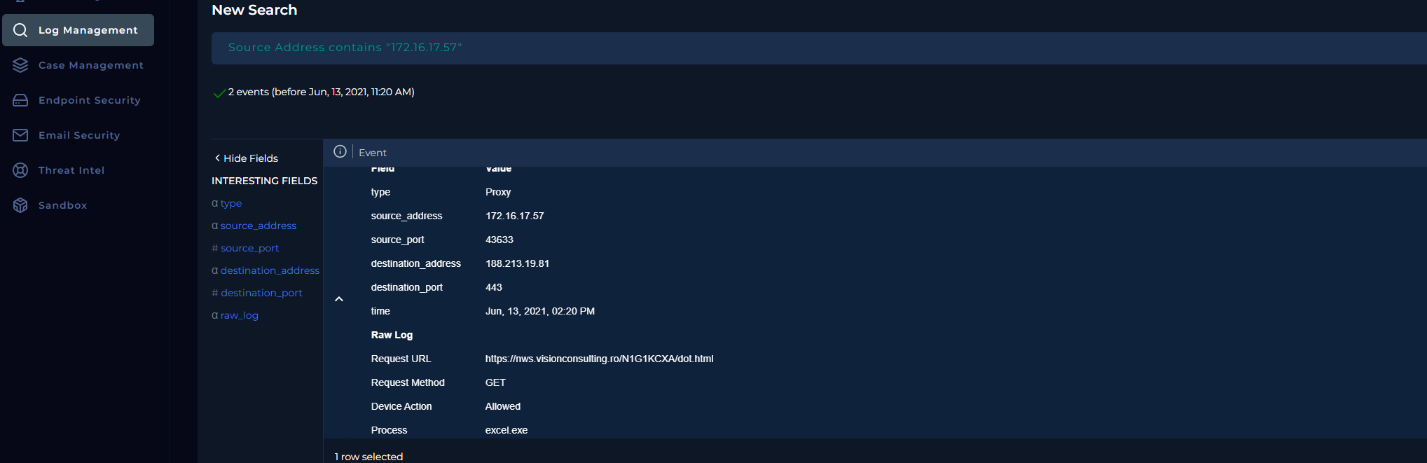
Based upon the image shown above of the email, there is an attachment present. Yes, will be my answer.



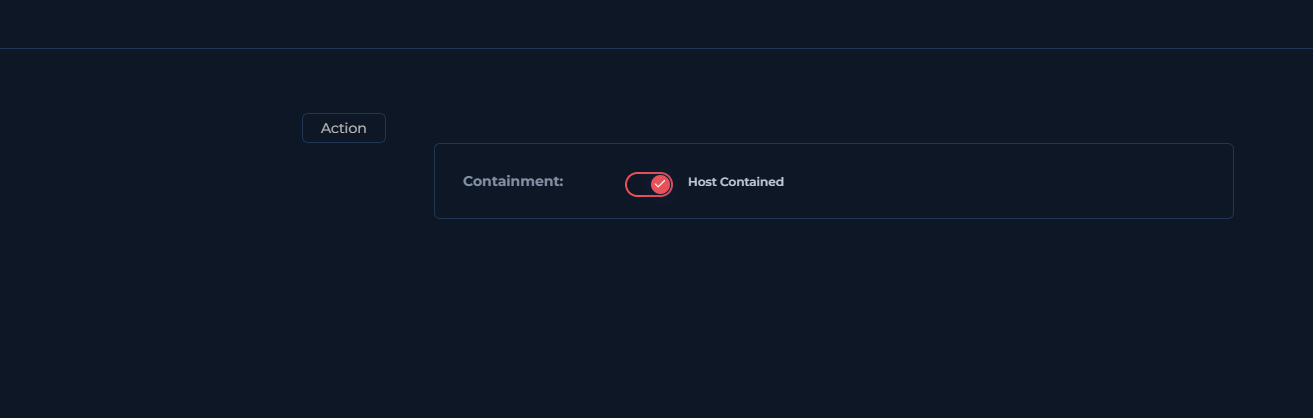
Before I could possibly open the file attached to the email, I was able to import the URL link into Virus Total and received negative results indicating the file has malware, which would harm my desktop if I was to install it.



I will be checking to see if the receiver of the email address Lars opened the email by gathering their IP address and looking into **Log Management**.



Within the log management, it shows that Lars has opened the same file listed above as malicious “nws.visionconsulting”



I have contained the device to prevent any further spread within the system.