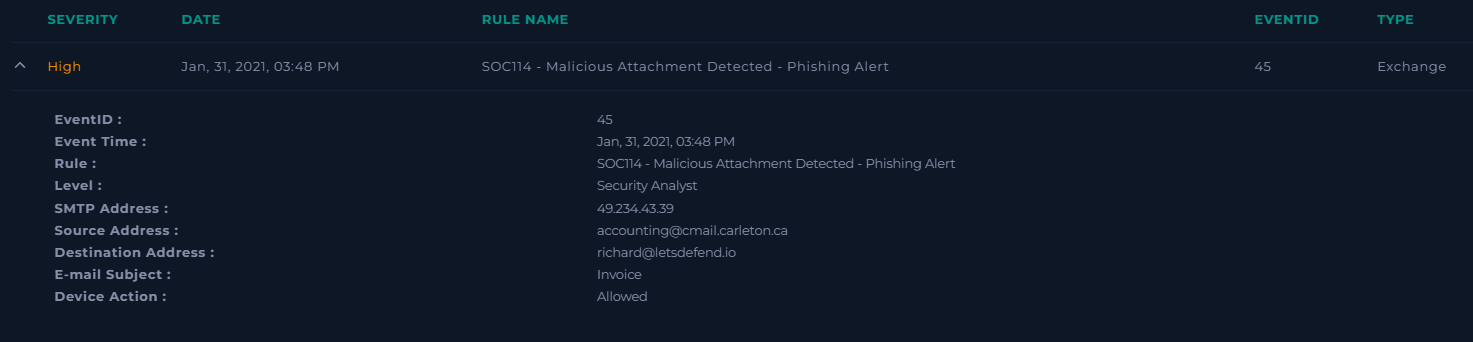
In this activity, I will investigate the ‘SOC114 - Malicious Attachment Detected - Phishing Alert’ on letsdefend.



When creating the playbook, I first gather general information about the alert.

When was it sent?

The email was sent at 3:48 PM on January 31, 2021.

What is the email's SMTP address?

The email's SMTP address is 49.234.43.39.

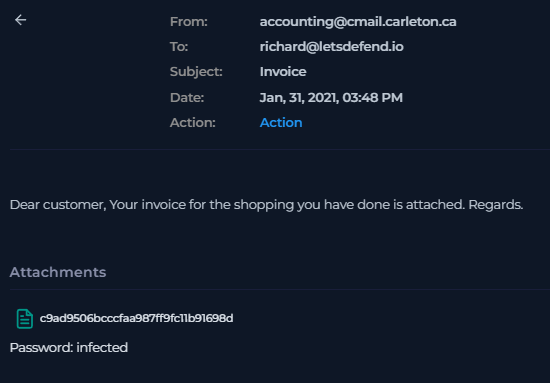
What is the sender address?

The sender’s address is ‘accounting@cmail.carleton.ca’.

What is the recipient address?

The recipient's address is ‘[richard@letsdefend.io](mailto:richard@letsdefend.io)’.

Looking at the contents of the email:



Is the mail content suspicious?

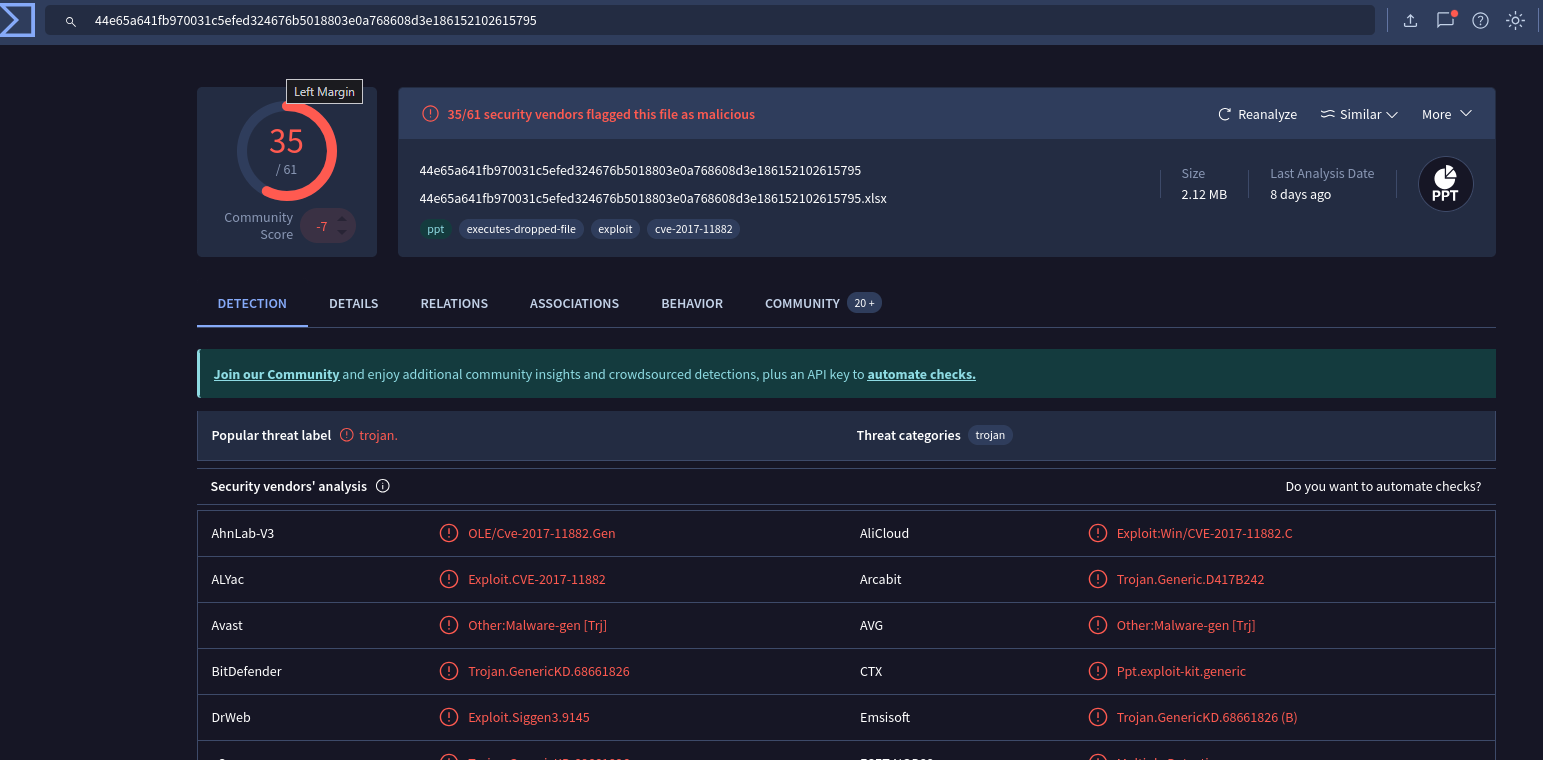
The email itself looks suspicious. The front address is concerning and the email attachment name isn’t very clear.

Are there any attachments?

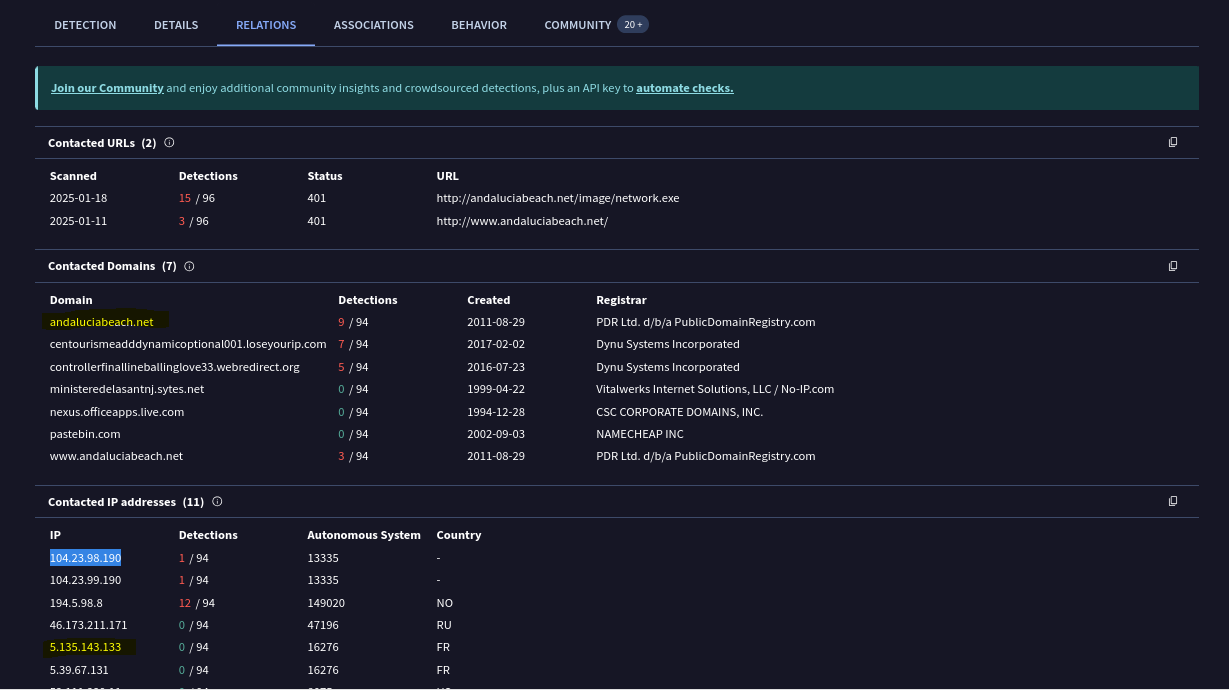
Yes

Next, I download this file into a remnux vm sandbox for analysis using the command:

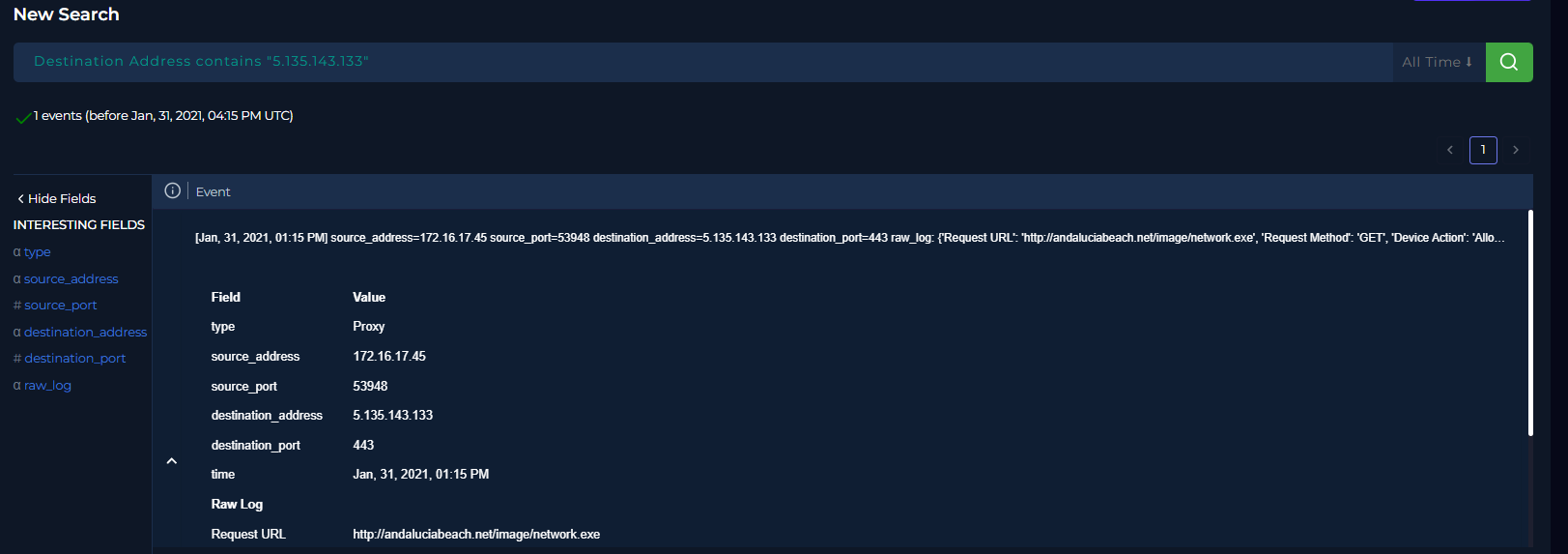
Unzip -P infected c9ad9506bcccfaa987ff9fc11b91698d.zip

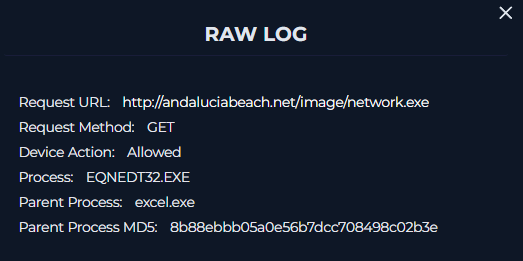
Running the extracted file through virus total showed many warnings, including identifying it as cve-2017–11882. This would allow an attacker to run arbitrary code in the context of the current user by failing to properly handle objects in memory, aka "Microsoft Office Memory Corruption Vulnerability".  


Under the relations, we find a few relations to check our logs for in case this malicious file was executed.

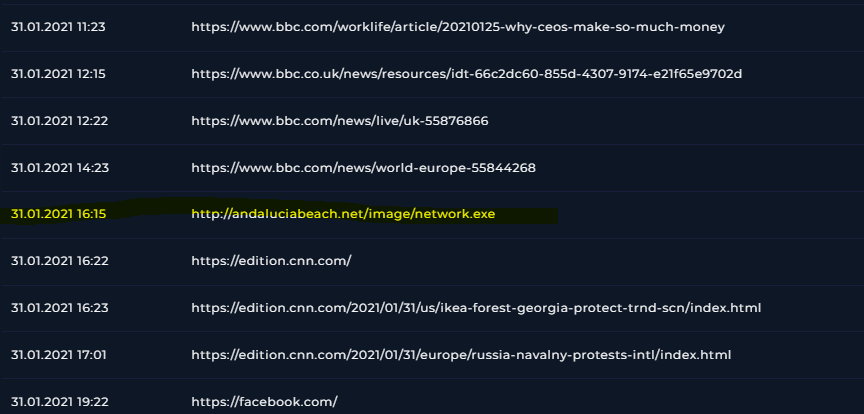


Within the logs we find a log that contains both the requested urll andaluciabeach.net and the destination address 5.135.143.133.

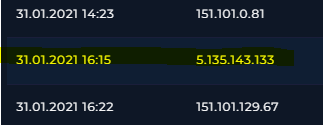


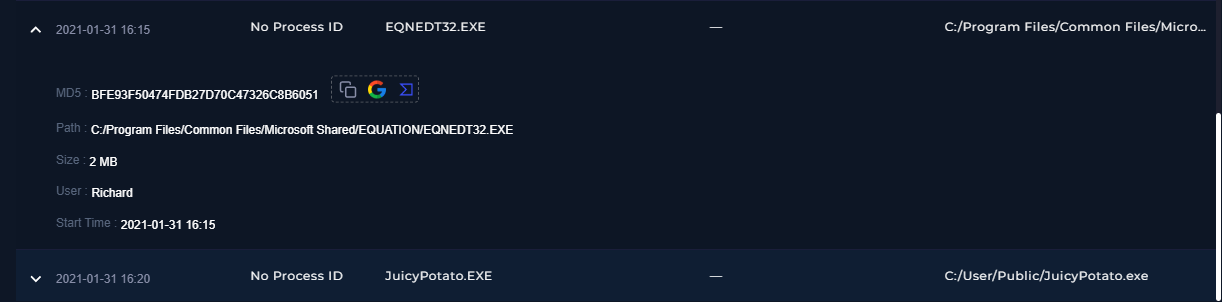


Using the source address 172.16.17.45 we find that the infected endpoint is RichardPRD. Searching Richard’s browser history after January 31, I find that he did visit the site January 31 around 4:15 PM.

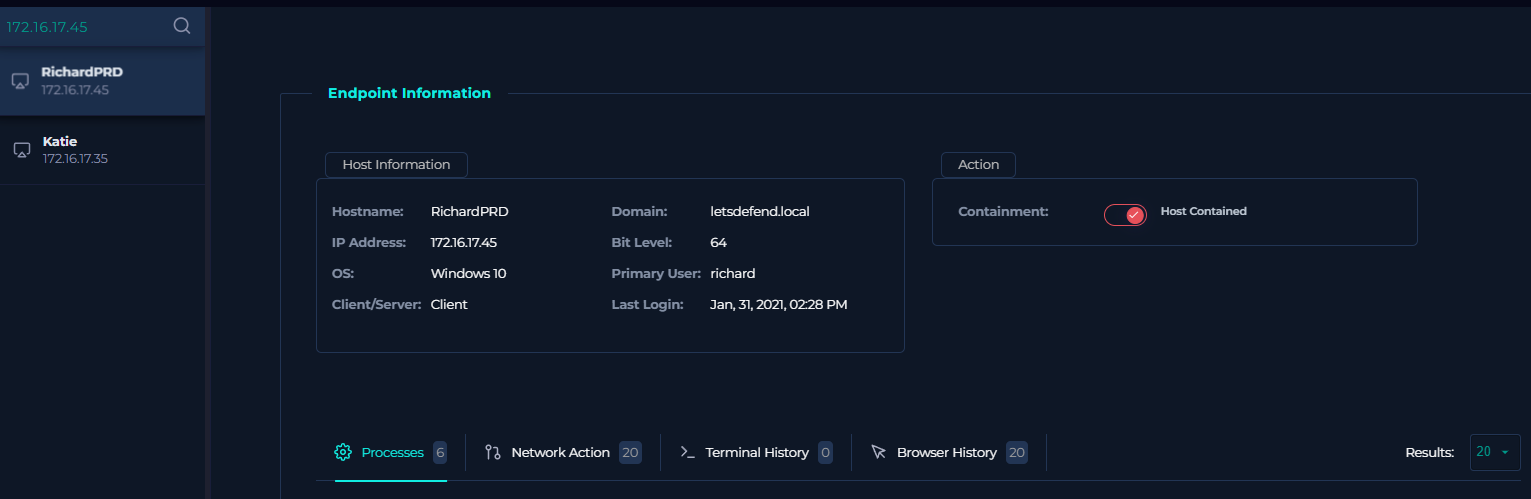


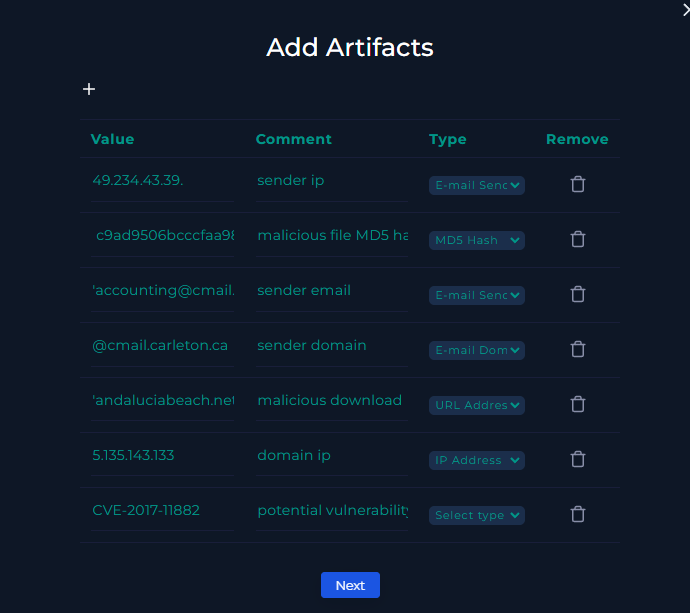
Looking inton the network actions, I saw a request for the connecting IP at the same time.



Within processes I see EQNEDT32.exe and JuicyPotatio.exe which can be used for privilege escalation.

As the user is running a malicious file and there's suspicious activity happening, I contain the endpoint.





Analysis note:

The malicious file was open which lead to a malicious domain execute cve-2017-11882. The affected system has been disconnected from the network.