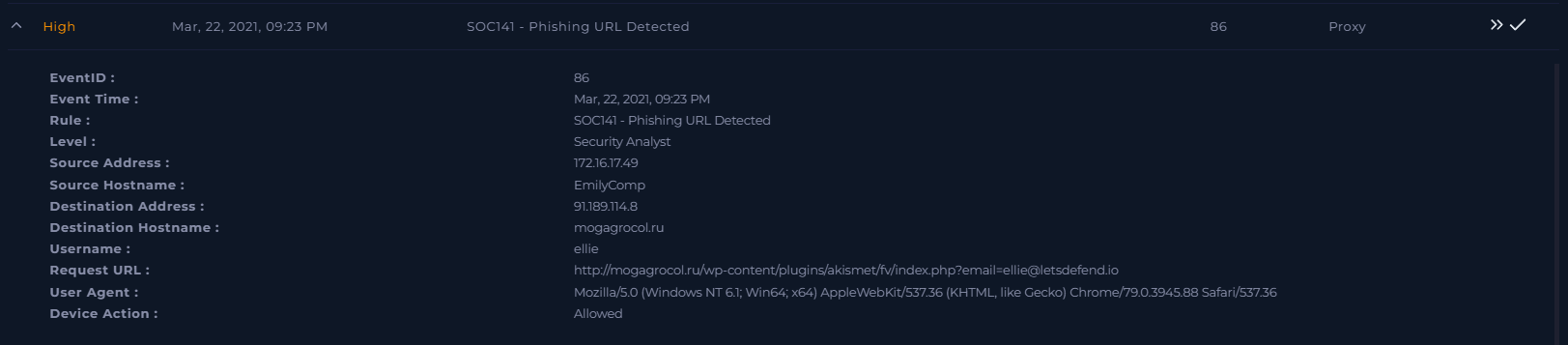
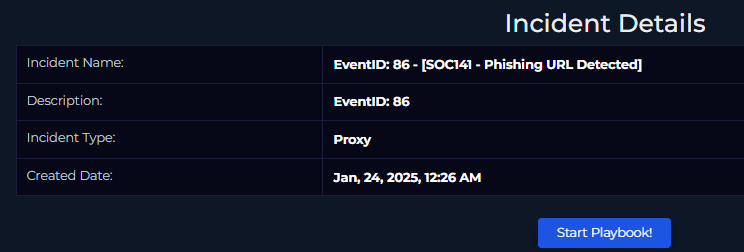
Within this exercise, I will investigate a phishing alert received in which a phishing URL was sent to a victim wanting them to open it.

Alert:



Now we will make a casebook on this alert.



From the alert we find that..

Source Address: 172.16.17.49

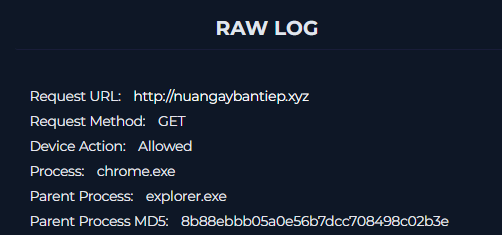
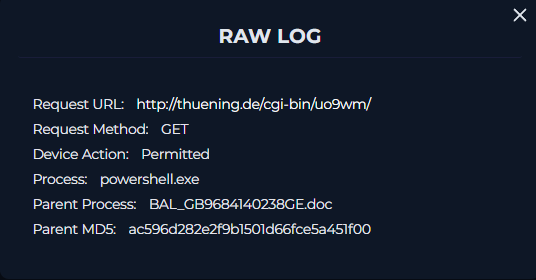
Destination Address: 91.189.114.8

User-agent: Mozilla, Windows

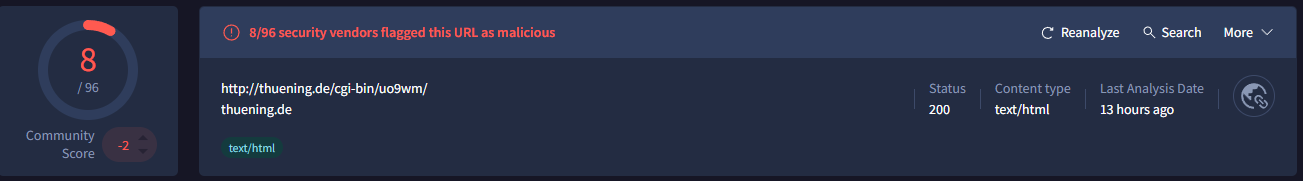
Using the log management tool I search the source address and find two alerts.



With in these alerts is the following information.



Analysing these two urls on different sites such as virustotal and urlhaus shows evidence of malware, showing that this is malicious.



Now I look into the log management tool to see if this file was accessed. Examining the logs above we find:

When was it accessed?

Apr, 04, 2021, 08:10 PM

What is the source address?

172.16.17.88

What is the destination address?

192.64.119.190

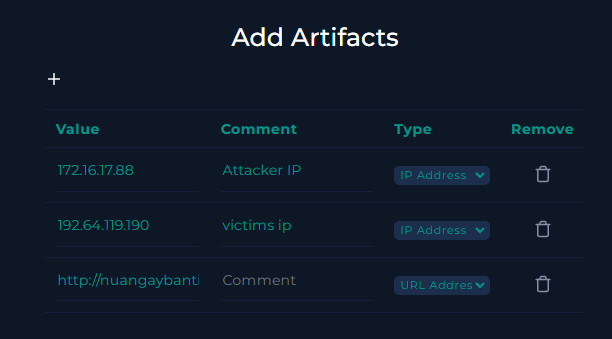
Which user tried to access?

Mark (found by searching IP on endpoint security)

What is the User Agent? Mozilla, Windows

Is the request blocked?

No



Analysis note:

This seems to be a true positive of a Trojan being spread via phishing email. The affected pc has been disconnected from the network.