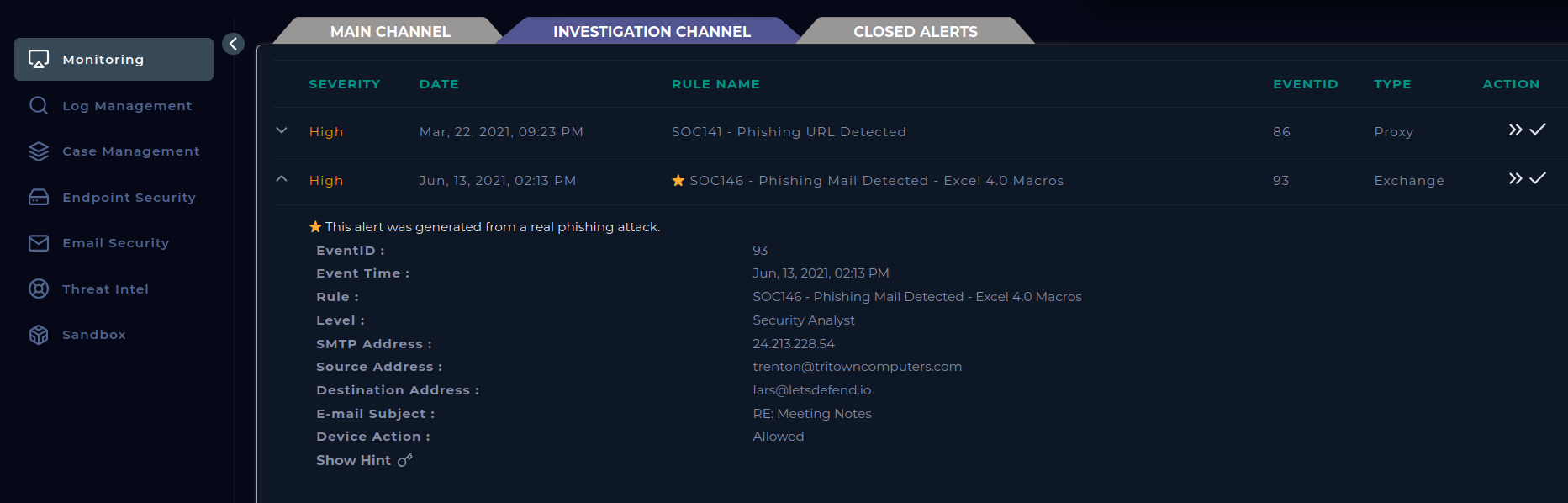
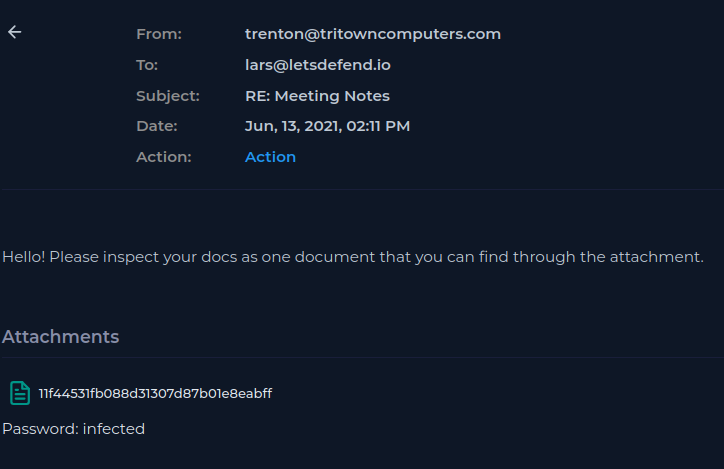
Phishing email SOC alert lab

According to the following alert, on June 13 2021 at 02:13 PM, we received an alert of a potential phishing attack.

When checking the alert we see that our endpoint user lars has received a suspicious file from [trenton@tritowncomputers.com](mailto:trenton@tritowncomputers.com).

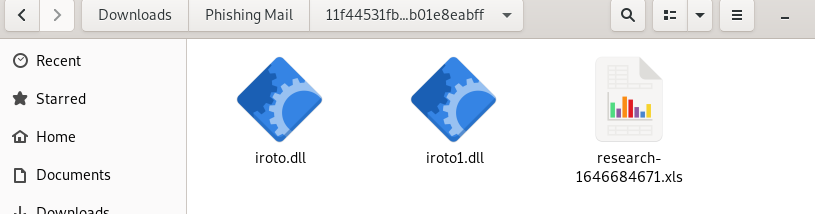


Searching in email security, we find a copy of the email that generated the alert.

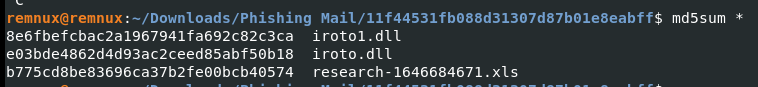


Next, I download this file into a remnux vm sandbox for analysis using the command:

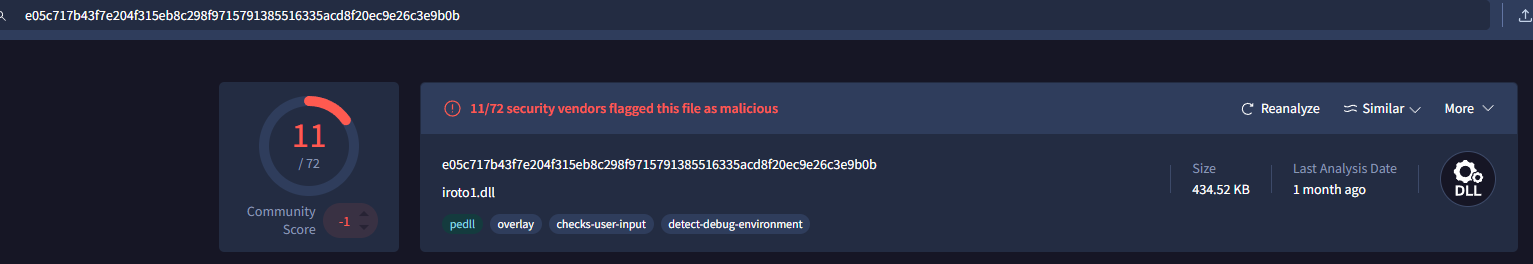
Unzip -P infected 11f44531fb088d31307d87b01e8eabff.zip

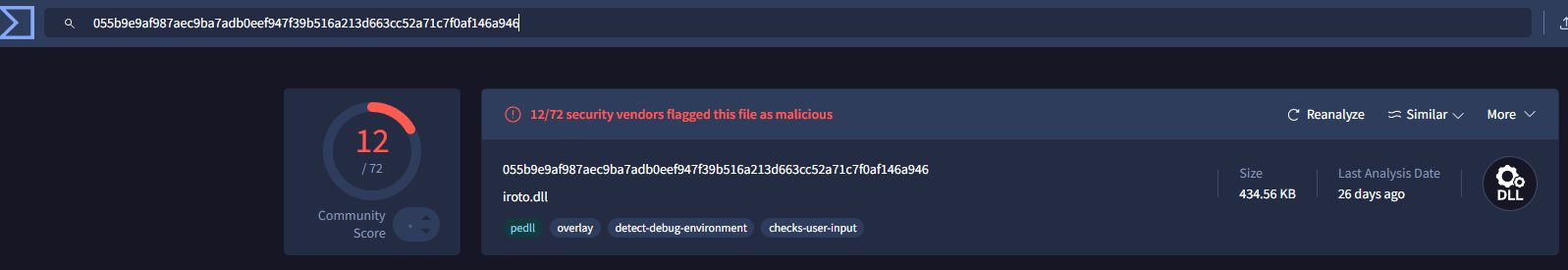


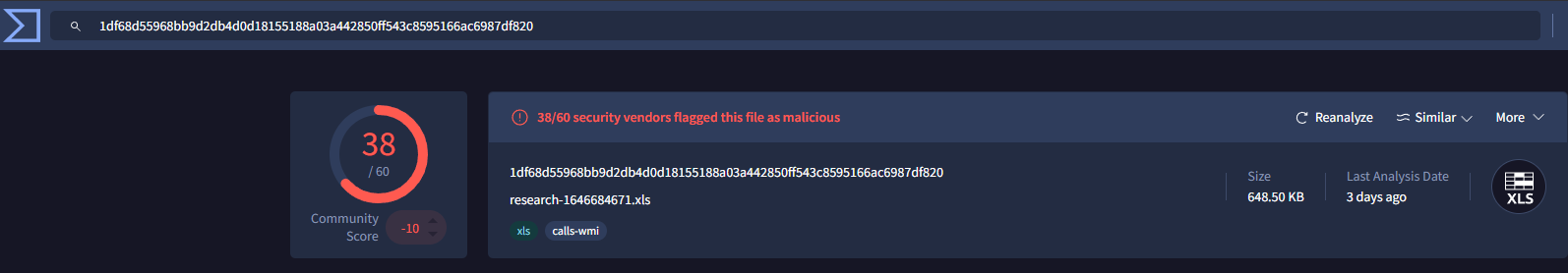
Using the renmux tool md5sum to calculate the hash of the files in the attachment. These hashes can be useful for identifying malware as they can act as a fingerprint for the malware.



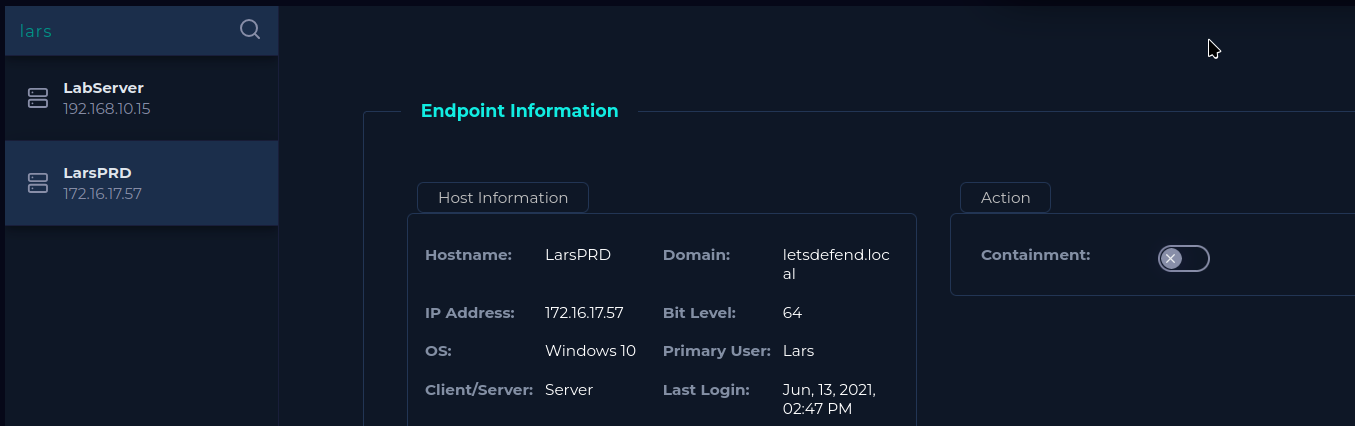
Taking these hashes and performing a hash search into virustotal, we find the three files are tagged as malicious. irotol .dll is detected as a trojan.



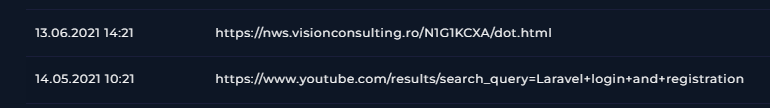




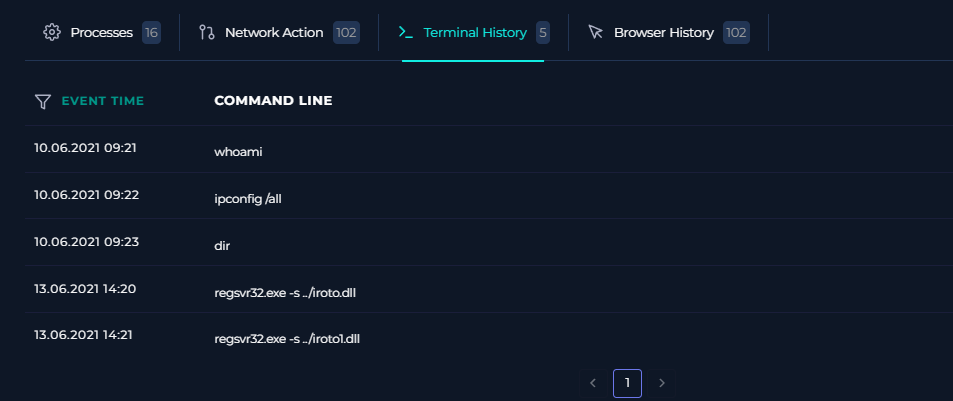
We know that the email was delivered to the user as the allert listed device action = allowed.

We need to know if the end user has opened this suspicious file. To find this information, we look into the endpoint logs for LarsPRD. 

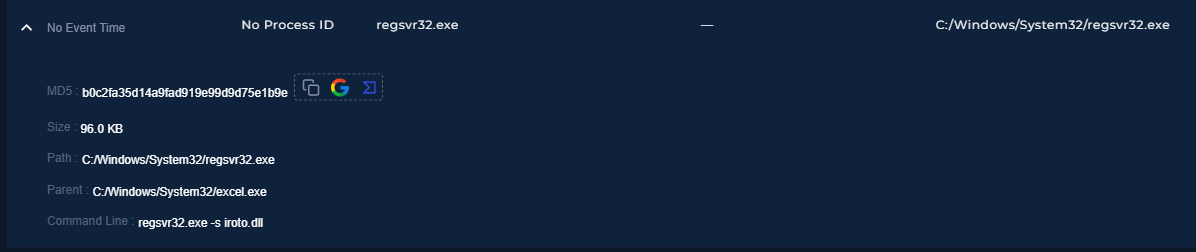
Within the browser history we find URLs of the malicious files matching with the time found on the alert.



During the same time we also see the command line history also shows the registration of malicious dlls.

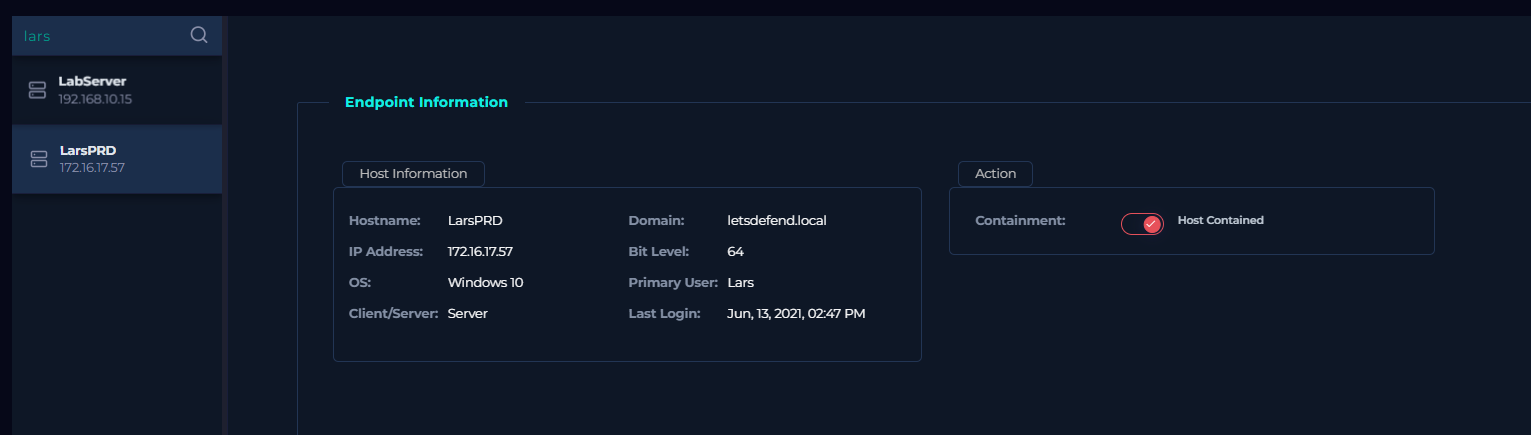


Despite not showing an event time, we see the excel process opening regsvr32.exe with the processes sharing the same MD5.

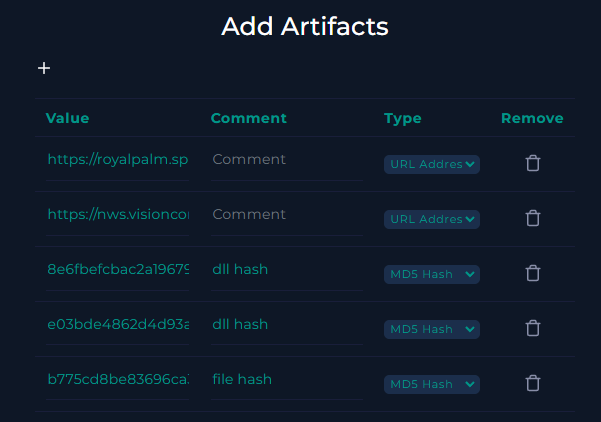


It can be safely considered that this malicious file was opened.

Lars endpoint must be immediately contained to avoid further damage.



In this analysis we found:



Conclusion:

Unfortunately we can see that the malicious file within the phishing email was successfully executed. This is along with evidence of regsvr32.exe being used to share malicious dlls. Lar machine was immediately contained in response.