Wanna cry is a ransomware that affects windows operating system and was used in May 2017. In order to analyse it, a sample was gotten from a github repository and analysed using 3 tools.

1. Any.run
2. Hybrid analysis
3. Virus total

A sample of was downloaded from <https://github.com/ytisf/theZoo/tree/master/malware>

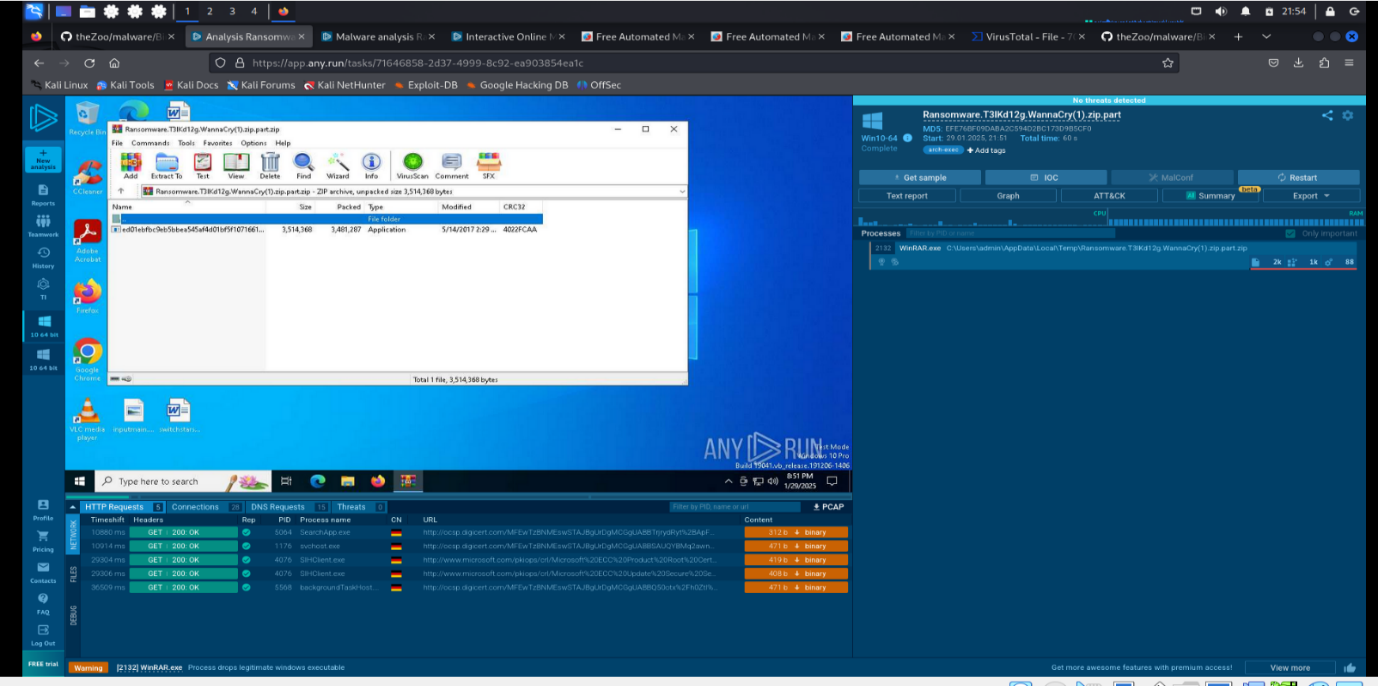
A screenshot of a computer

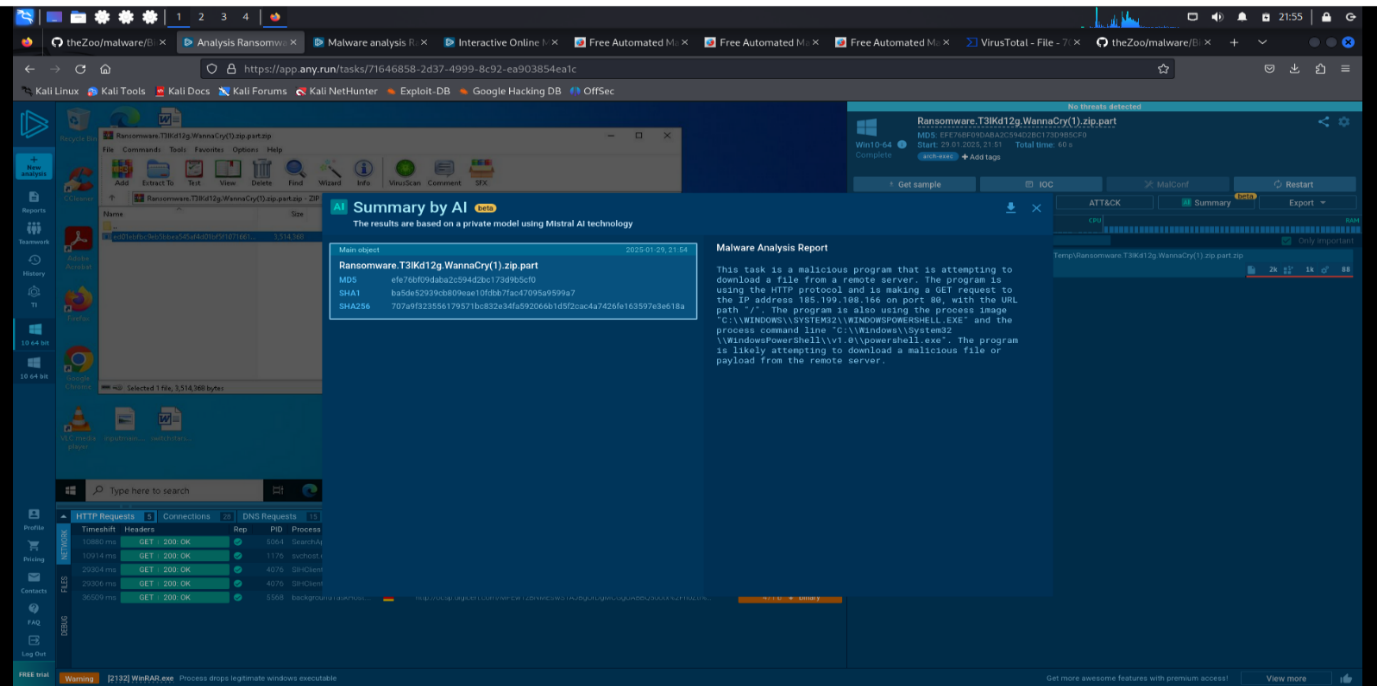
Description automatically generated

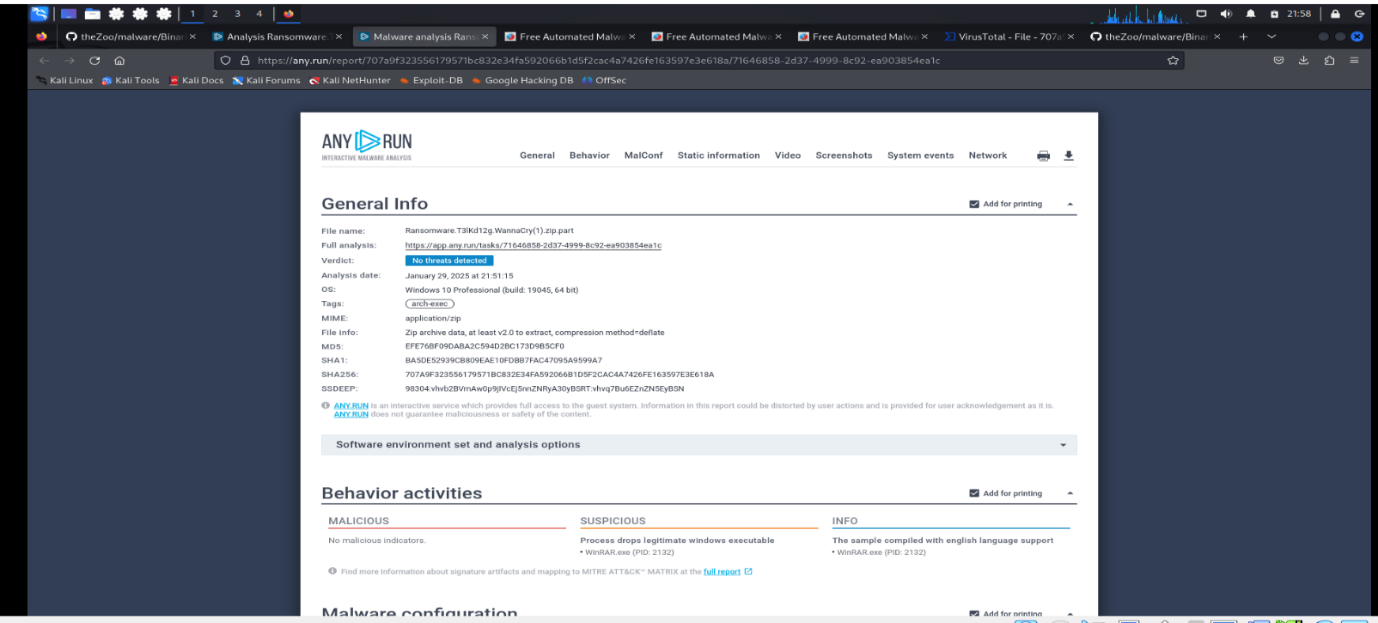
The downloaded sample was uploaded to any.run. Any run is a malware analysis platform that create any type of environment in a sand box. Windows 10 was chosen for the analysis.

A computer screen shot of a computer screen

Description automatically generated







According to anyrun, the file is a ransomeware and is attempting to download a melicious file from a remote sever.

* It tried to execute the program “WinRAR exe (PID: 2132)”
* It carried out 1636 events, 1628 read events and 8 write events
* It had 5https request, 28TCP/UCP connections, 15 DNS requests

The file was the uploaded on virus total for further analysis.

According to virus total

* it is a trojan ransomware of the family genericfca
* 14 out of 66 security vendors flagged it as malicious
* Its been called several names over the years such as “ Ransomware.WannaCry.zip, SpongebobScreenToy.zip, insta@meta.zip.”

A screenshot of a computer

Description automatically generated

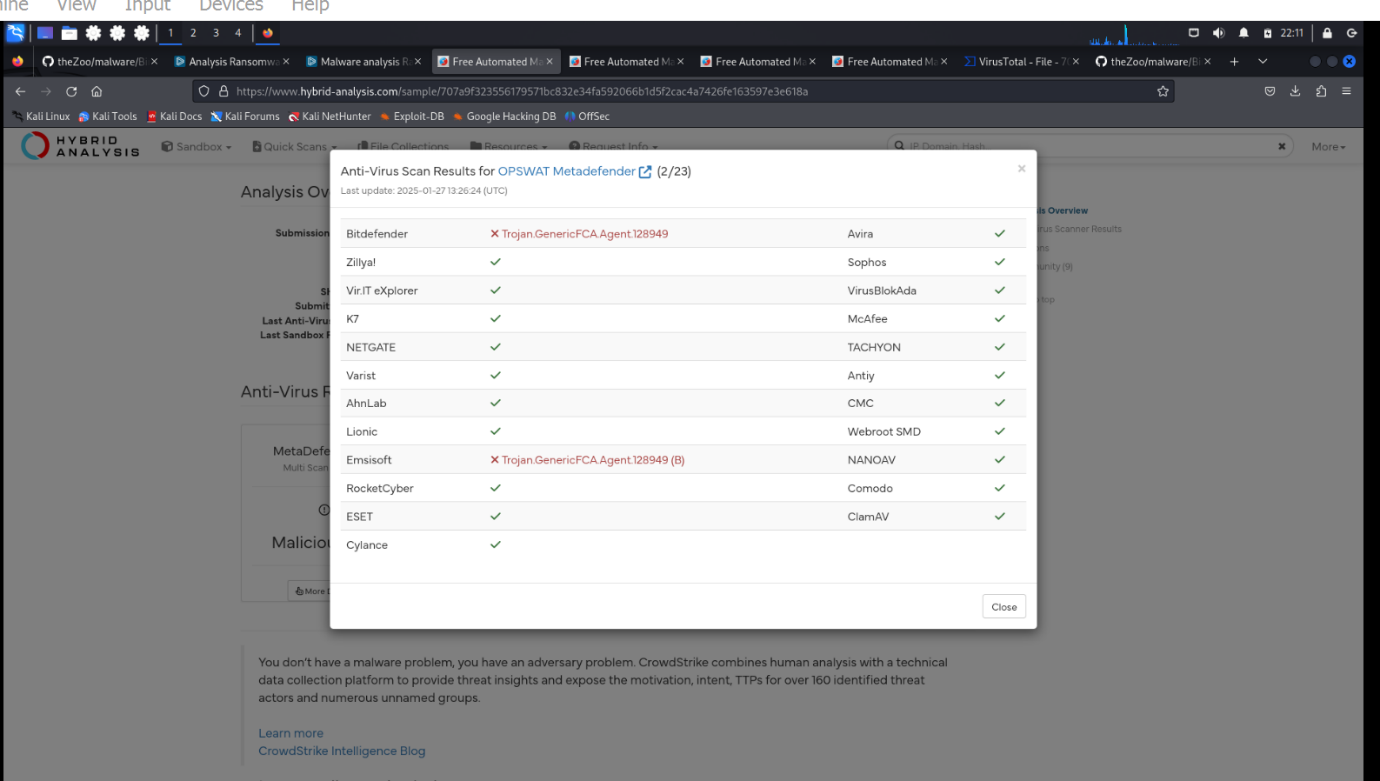
A screenshot of a computer program

Description automatically generated

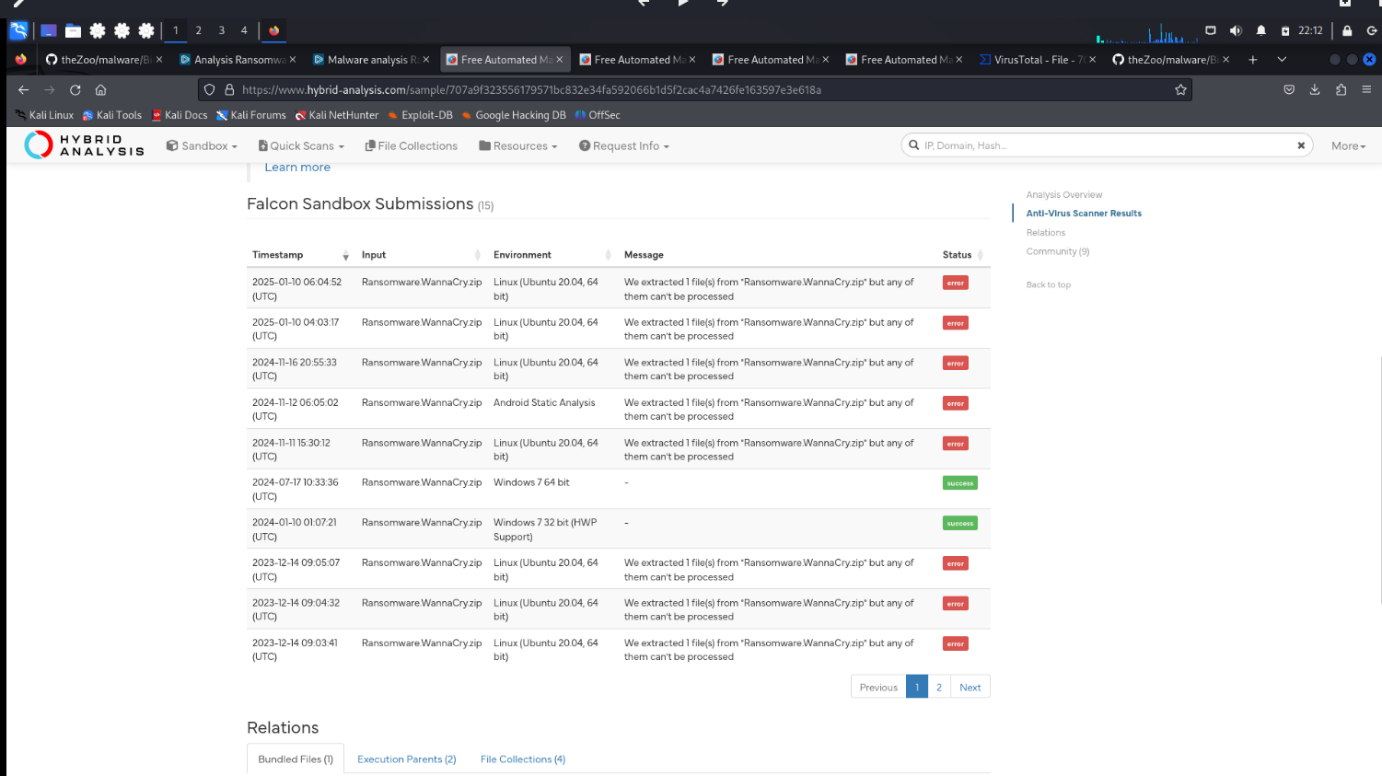
A screenshot of a computer

Description automatically generated

Lastly, the malware was analysed with hybrid analysis which does both static and dynamic analysis. On hybrid analysis only bitdefender and Emsisoft flagged the ransomware.



Hybrid analysis using falcon sandbox showed the virus only affects windows O.S



It also tried to execute several malicious files as well as connect to different hosts

