Remote Working [Let's Defend – Write-up]

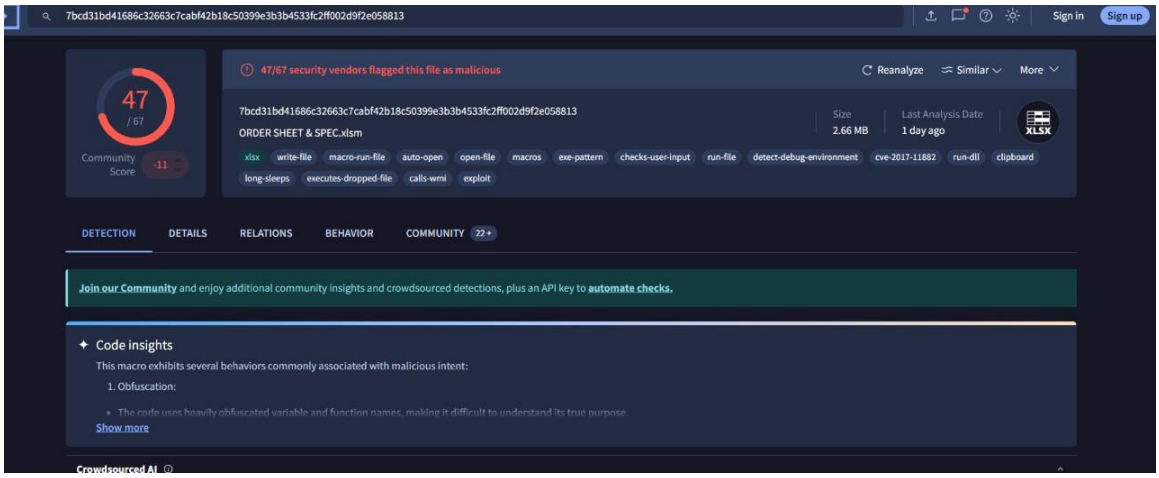
Analysis XLS File

File link: /root/Desktop/ChallengeFiles/ORDER_SHEET_SPEC.zip
Password: infected

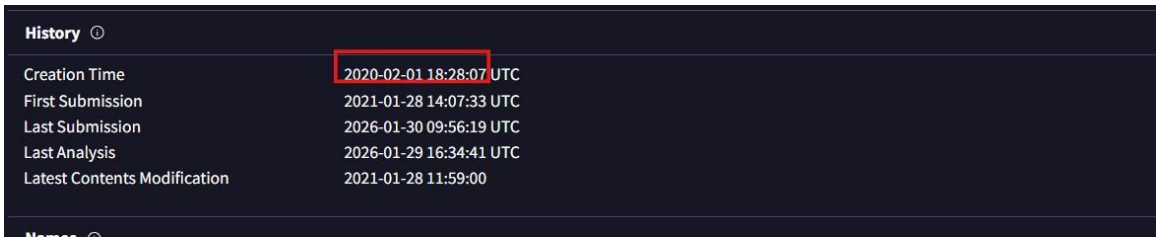
| Start investigation

First, I want to calculate the hash so I can search on virstotal.

```
root@ip-172-31-14-26:~/Desktop/ChallengeFiles# sha256sum 'ORDER SHEET & SPEC.xlsm'
7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813  ORDER SHEET & SPEC.xlsm
root@ip-172-31-14-26:~/Desktop/ChallengeFiles#
```



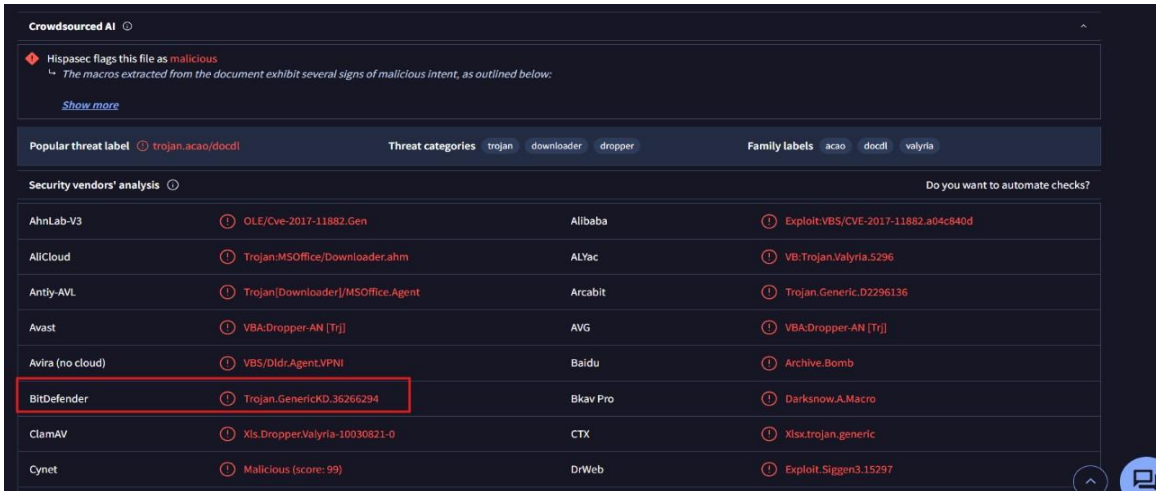
Q1: What is the date the file was created? (UTC) Answer Format: YYYY-MM-DD HH:MM:SS



Go to Details after that see the History.

Answer: 2020-02-01 18:28:07.

Q2: With what name is the file detected by Bitdefender antivirus?



In Home page of Virstotal I get the answer.

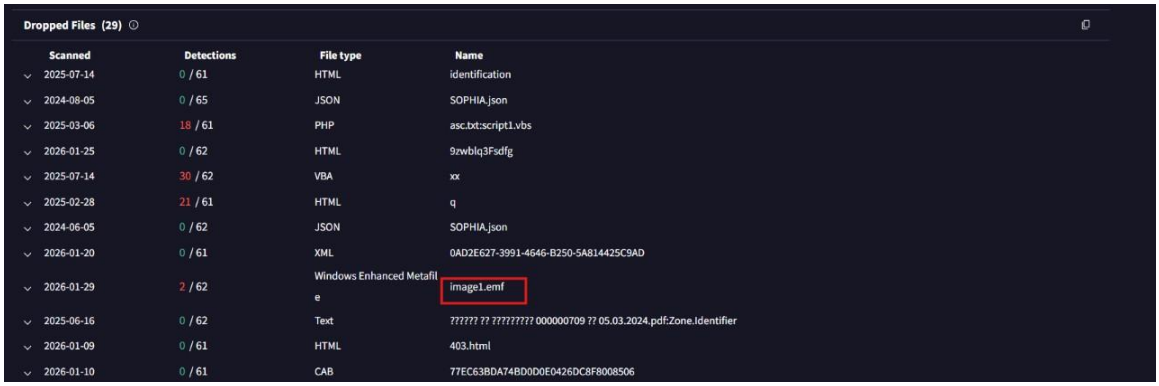
Answer: trojan.generickd.36266294

Q3: How many files are dropped on the disk?

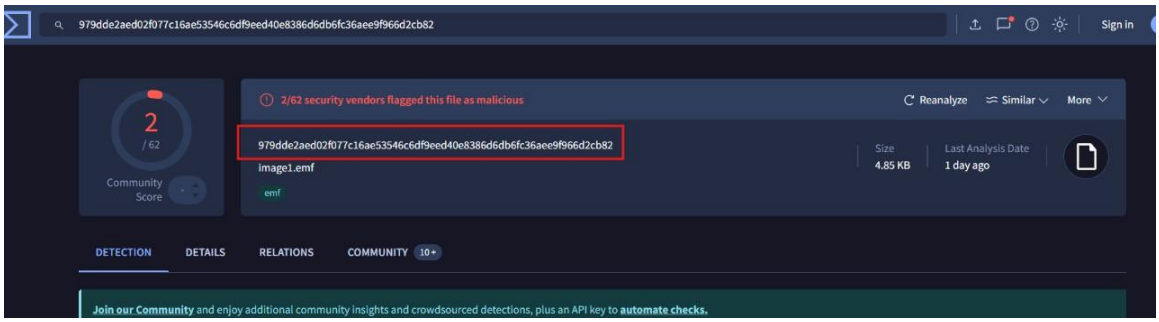
Go to Details after that see the Dropped Files above the Total.

Answer: 29

Q4: What is the sha-256 hash of the file with emf extension it drops?



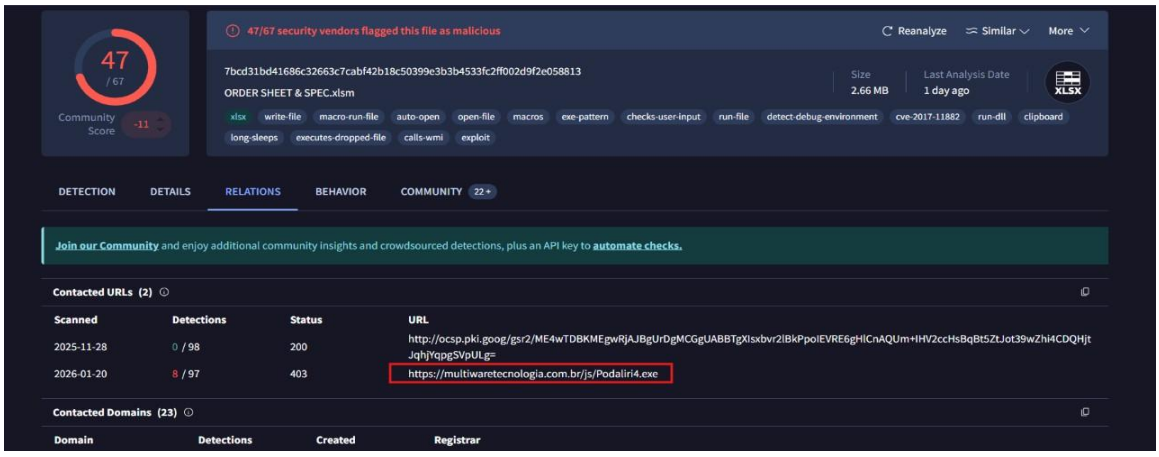
in drooped files just click on it after that you will get the hash above.



Answer: 979dde2aed02f077c16ae53546c6df9eed40e8386d6db6fc36aee9f966d2cb82

Q5: What is the exact url to which the relevant file goes to download spyware?

Go to Relations after that you will see the Url



Answer: https://multiwaretecnologia.com.br/js/podaliri4.exe

Summary

This investigation into the ORDER_SHEET_SPEC sample was highly educational and greatly improved my malware analysis workflow. It taught me how to effectively pivot between VirusTotal's tabs to extract deep forensic details, such as tracking file creation history and identifying specific antivirus detections like Bitdefender’s Trojan labels. I also gained practical experience in mapping out the 'Dropped Files' section to find specific artifacts, such as the .emf file and its SHA-256 hash.