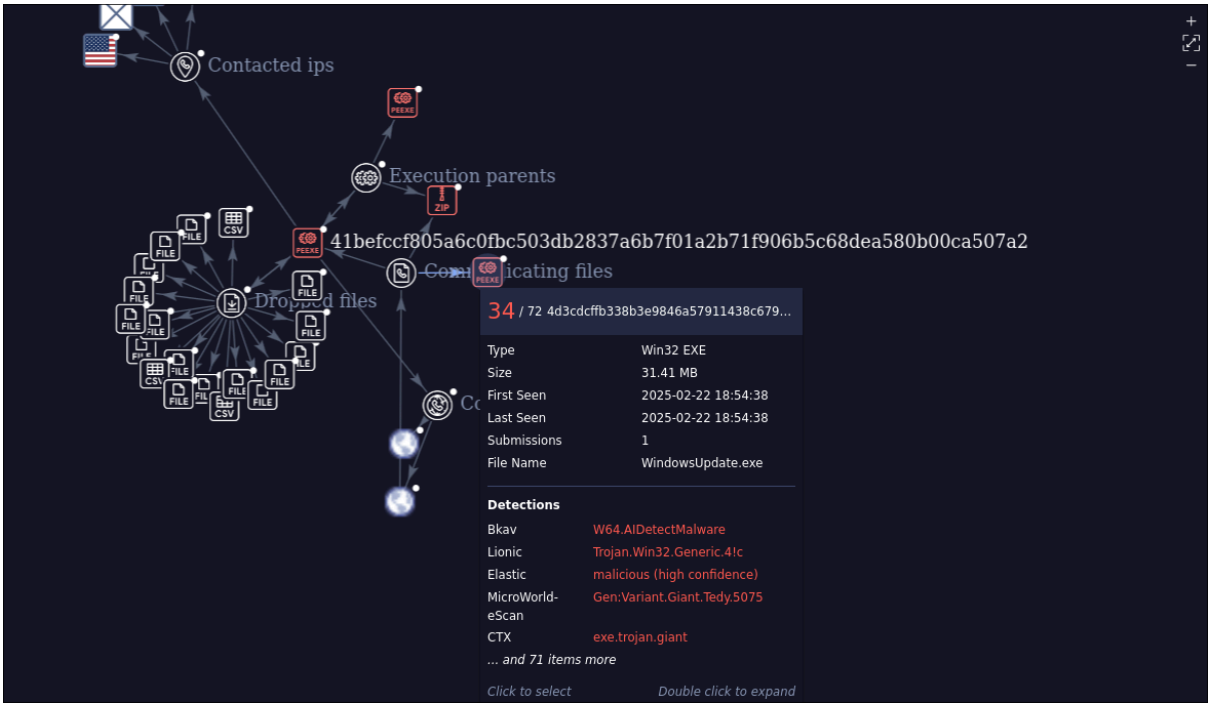
Because it’s an OSINT challenge, I uploaded the file on VirusTotal to search for some information about this malware (hint : **This task is "real malware". Sometimes the "information" you need may not exist directly in that "binary".**)

The challenge was solved on a Linux machine, it’s hard on Windows because of the antivirus.

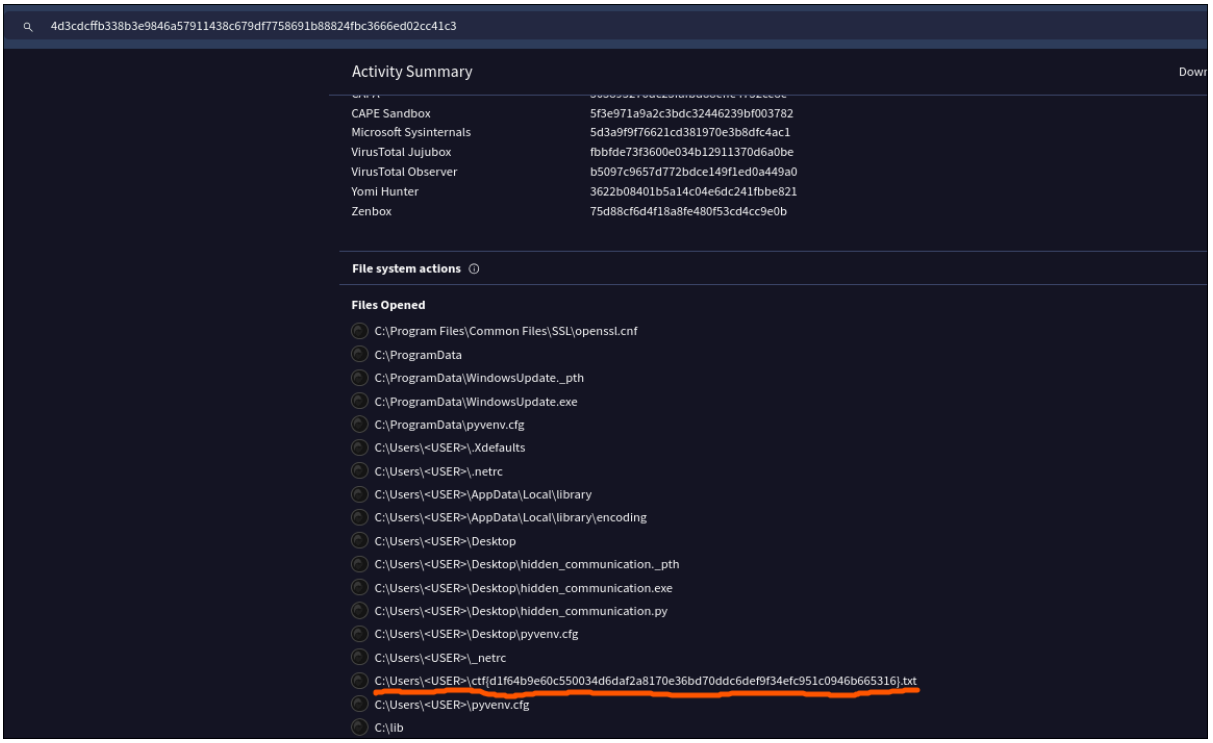
The requirement instructs us that we need to find a malware file related to **hiddendot.exe.** I searched up Github pages, Malware bazaar page, LinkedIn pages, but nothing. After that, I went back to VirusTotal, created my account and went to Relations -> Graph Summary, where I got this schema :

An interesting thing I noticed was the **stim-comunity.ro** page, where I wanted to see the communication files.

Here, I found a file that was almost the same size as the original file, so I copied its sha256 and went to virustotal



So, on the following page : https://www.virustotal.com/gui/file/4d3cdcffb338b3e9846a57911438c679df7758691b88824fbc3666ed02cc41c3, we can find the flag at Behavior -> Files Opened :



THE FLAG : ctf{d1f64b9e60c550034d6daf2a8170e36bd70ddc6def9f34efc951c0946b665316} ~Z4que