

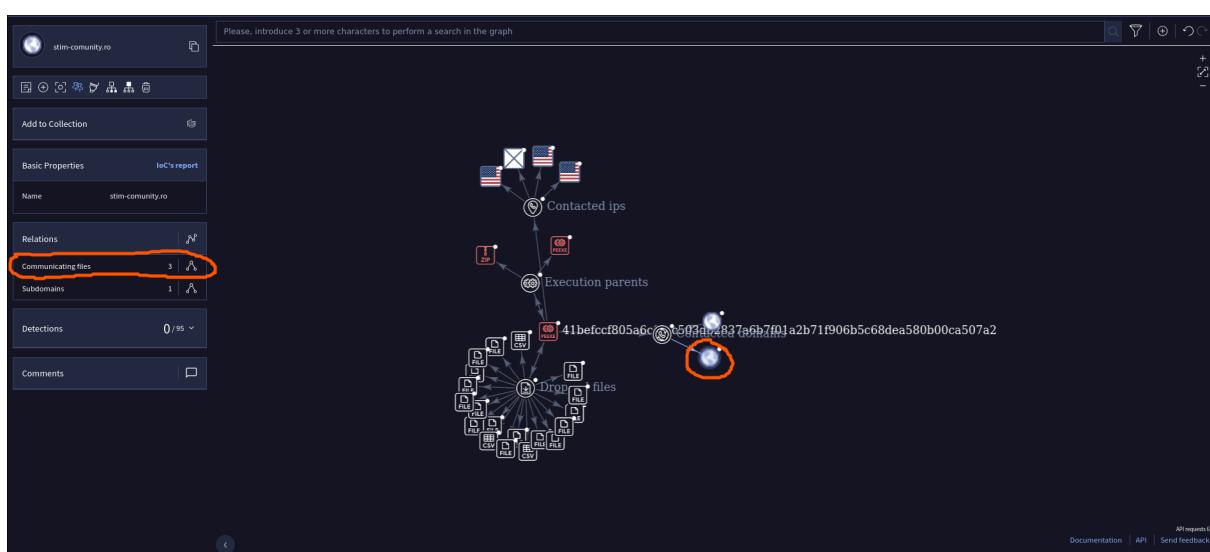
Because it's an OSINT challenge, I uploaded the file on VirusTotal to search for some information about this malware (hint : **This task is "real malware". Sometimes the "information" you need may not exist directly in that "binary".**)

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-community.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/4d3cdcffb338b3e9846a57911438c679df7758691b88824fbcc3666ed02cc41c3>, we can find the flag at Behavior -> Files Opened :

Activity Summary

CAPE Sandbox	5f3e971a9azc3bdc32446239bf003782
Microsoft Sysinternals	5d3a99f7f6621cd381970e3b8dfc4ac1
VirusTotal Jujubox	fbfbde73f3600e034b12911370d6a0be
VirusTotal Observer	b5097c9657d772bdc149f1ed0a449a0
Yomi Hunter	3622b08401b51a1c04e6dc241bbe821
Zenbox	75d88cf6d4f18a8fe480f53cd4cc9e0b

File system actions ⓘ

Files Opened

- C:\Program Files\Common Files\SSL\openssl.cnf
- C:\ProgramData
- C:\ProgramData\WindowsUpdate_.pth
- C:\ProgramData\WindowsUpdate.exe
- C:\ProgramData\pyvenv.cfg
- C:\Users\<USER>\.Xdefaults
- C:\Users\<USER>\.netrc
- C:\Users\<USER>\AppData\Local\library
- C:\Users\<USER>\AppData\Local\library\encoding
- C:\Users\<USER>\Desktop
- C:\Users\<USER>\Desktop\hidden_communication_.pth
- C:\Users\<USER>\Desktop\hidden_communication.exe
- C:\Users\<USER>\Desktop\hidden_communication.py
- C:\Users\<USER>\Desktop\pyvenv.cfg
- C:\Users\<USER>\.netrc
- C:\Users\<USER>\ctf{d1f64b9e60c550034d6daf2a8170e36bd70ddc6def9f34efc951c0946b665316}.txt
- C:\Users\<USER>\pyvenv.cfg
- C:\lib

THE FLAG :

ctf{d1f64b9e60c550034d6daf2a8170e36bd70ddc6def9f34efc951c0946b665316}
 ~Z4que