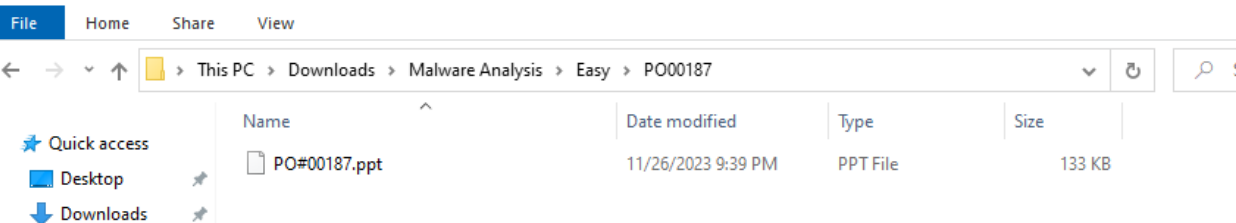


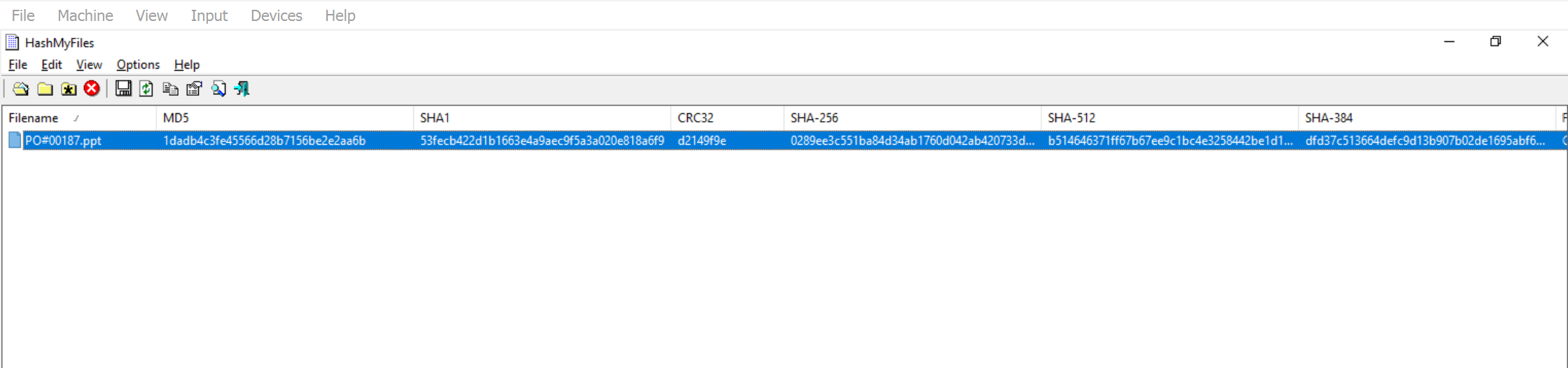
PS: The below analysis is done without looking at the writeups. Challenges by “Lets Defend”

**STATIC ANALYSIS**

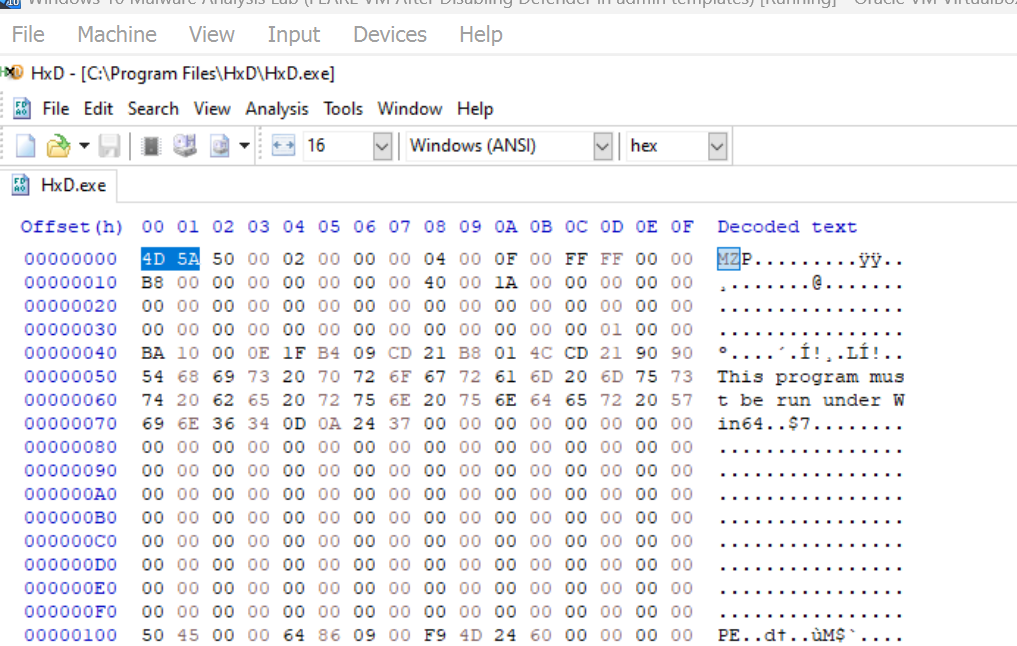
Downloaded the Malware on VM

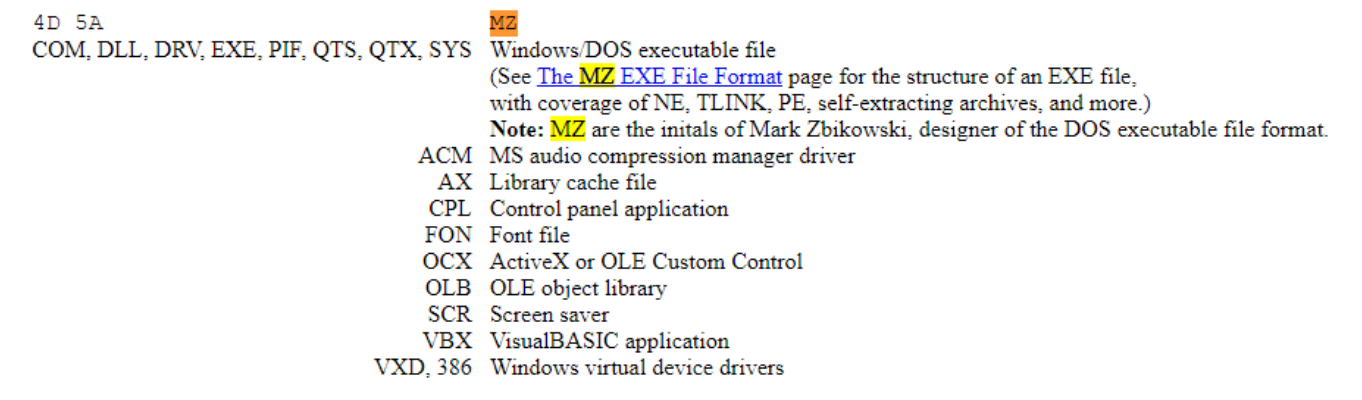


Identified Hash



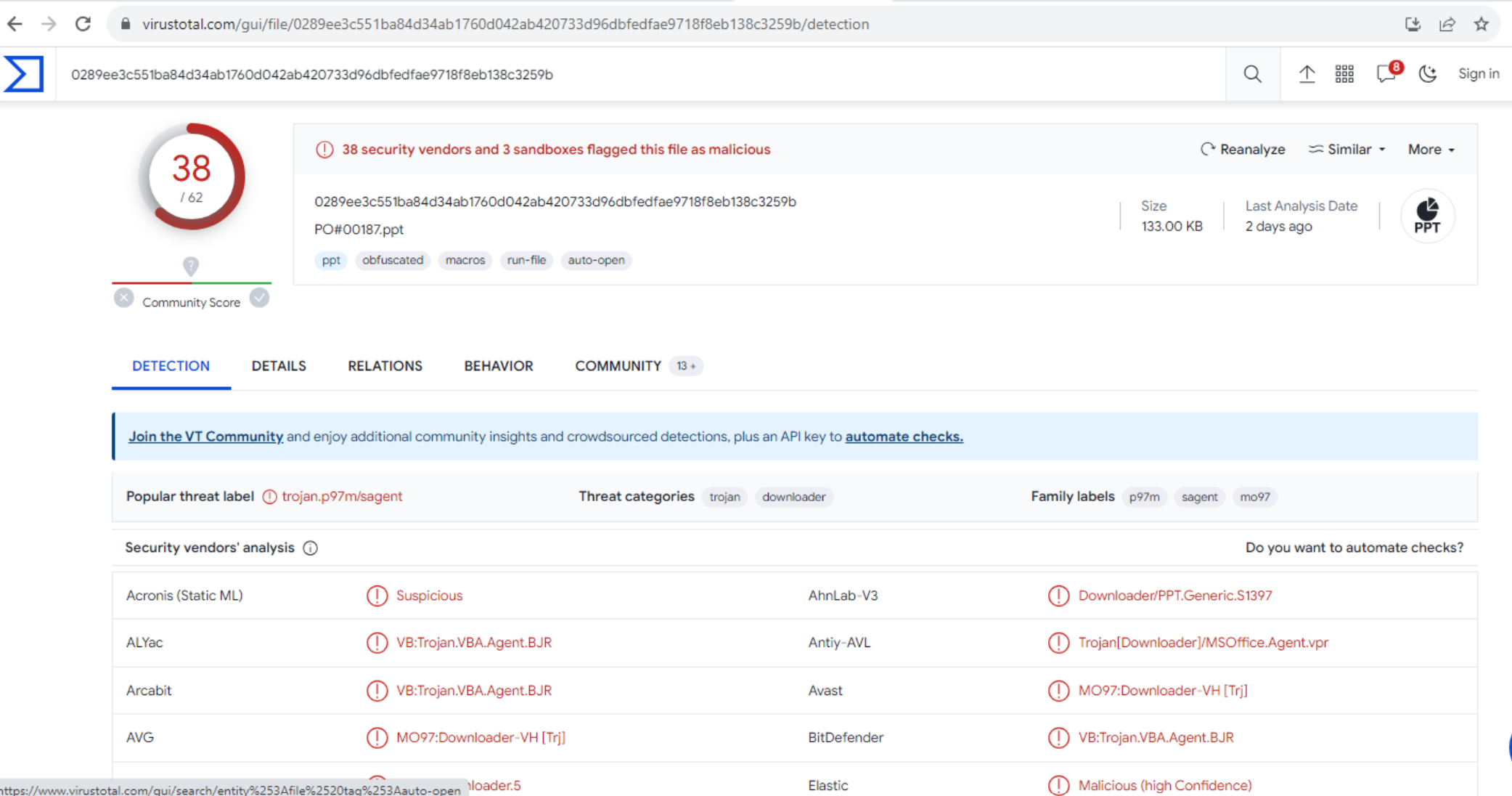
Verifying file type if its an executable or not. Files having 4D5A are executable files



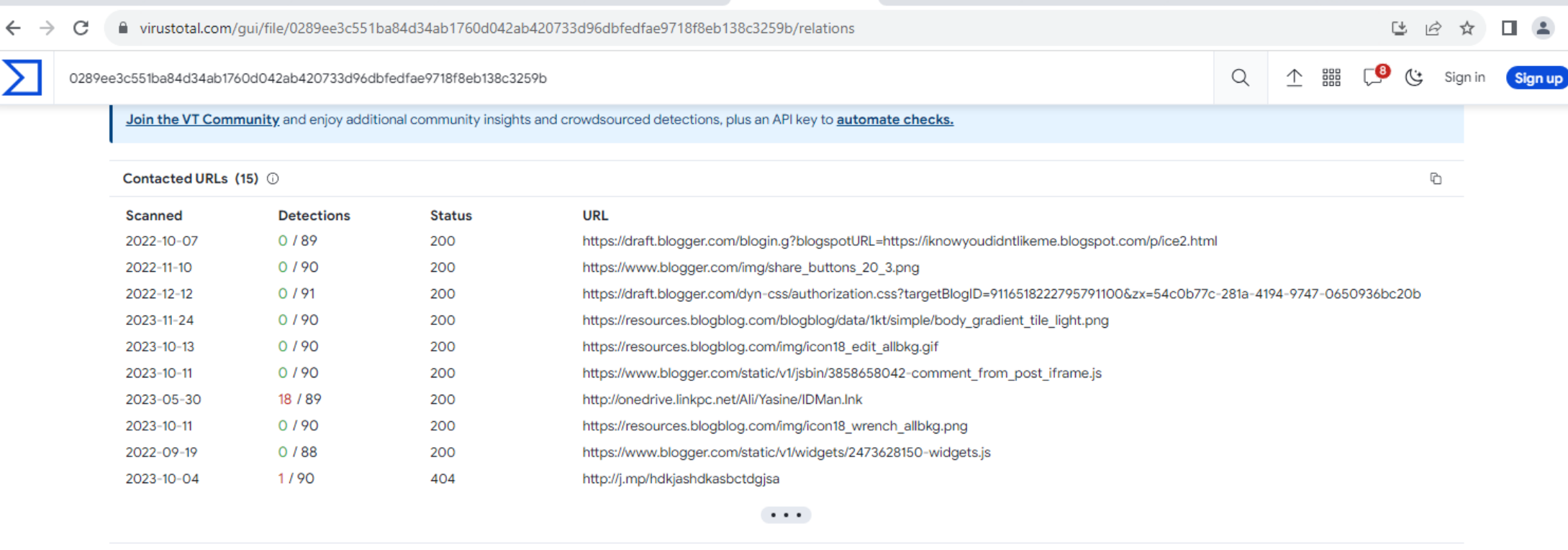


Gary Kessler’s file signature above

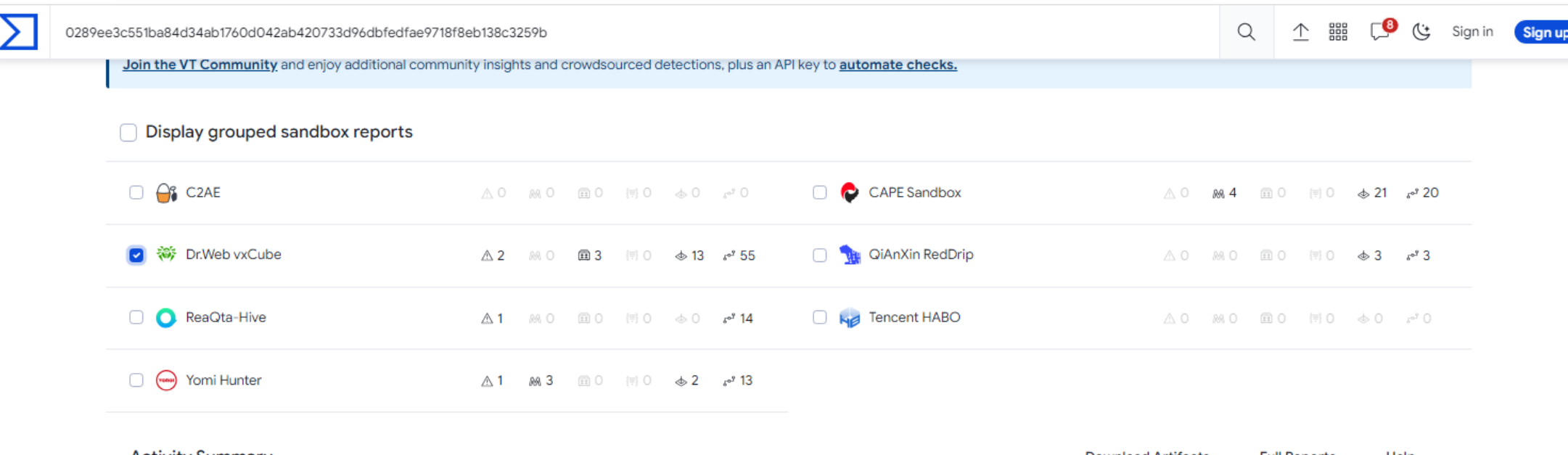
Verifying the hash in “virustotal” to identify the type of malware



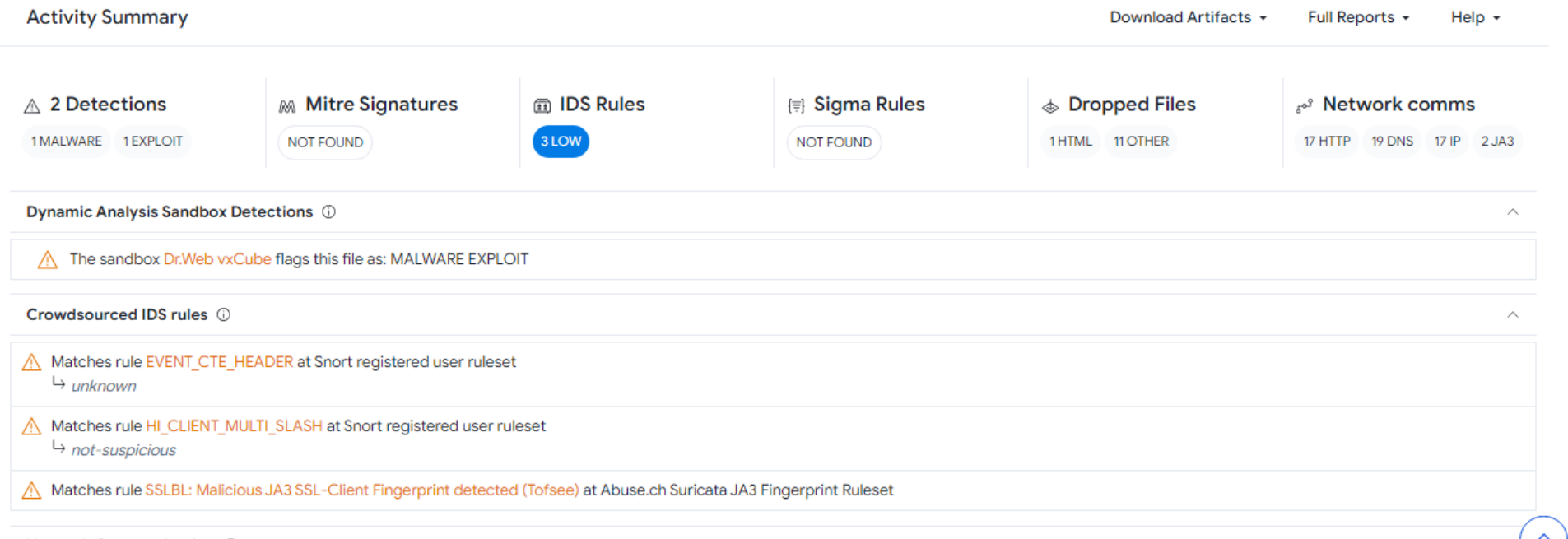
List of URLs the malware attempted to connect.



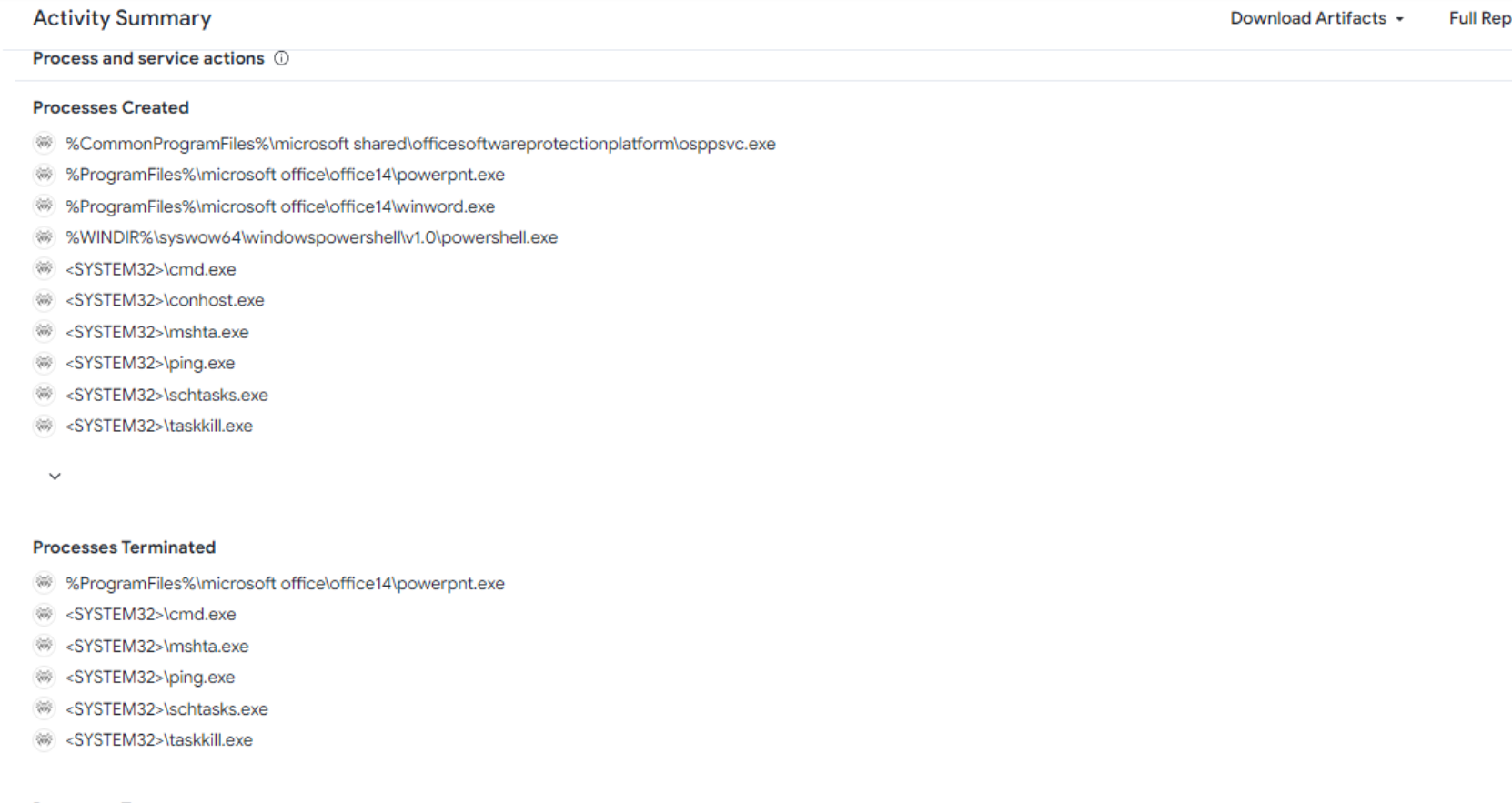
Sandboxes with their feedback, look out for IDS RULES(Dr.Web) that could have caught this virus

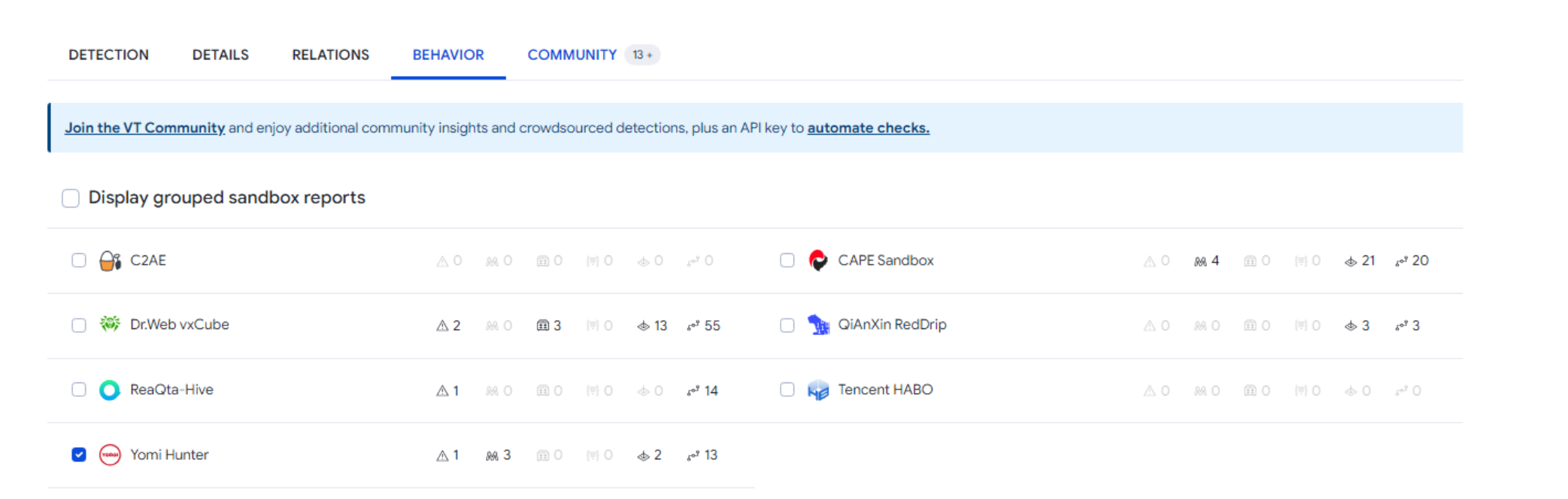


IDS rules that would identify the malware



List of process created, the schtasks.exe is creating a scheduled task for persistence





Files dropped by the malware locally in the computer. Identified by Yomi Hunter sandbox

