Static analysis:
Get sha256sum:
sha256sum.exe {Name of malware file.exe}

Get md5sum:
md5sum.exe {Name of malware file.exe}

virustotal.com score: 57/74 vendors flagged this as malicious
Trojan, downloader, ransomware

Extract static strings: floss command Pulls out arrays of characters that are greater than 4 characters and deobfuscates them.

- URLDownloadToFileW method found: malapi.io shows all potential malicious api calls
- InternetOpenURLA
- ShellExec
- Unicode (Bash) strings found:

FLOSS static Unicode strings:

Cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"
[http]://ssl-6582datamanager[.]helpdeskbros[.]local/favicon.ico
C:\Users\Public\Documents\CR433101.dat.exe
Mozilla/5.0
[http]://huskyhacks[.]dev
Ping 1.1.1.1 -n 1 -w 3000 > Nul &
C:\Users\Public\Documents\CR33101.dat.exe
open

PEStudio:
MZ found in code: Windows executable
This program cannot be run in DOS mode
Compile time found in file-header: Sat Sep 04 18:11:12 2021 | UTC

- If the time stamp says a date in 1992: it was made in Delphi

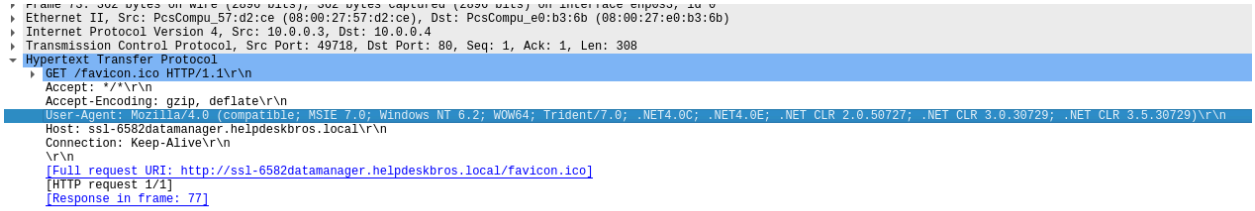
Virtual and actual binary size value is roughly the same

Dynamic analysis:

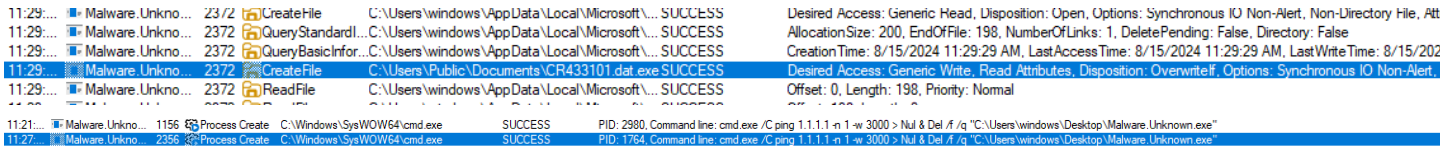
Internal detonation:

- CMD window, no other indicators
- Killswitch present, if no internet connection. Deletes itself from disk.

Network signatures:



Host signature:



Program Execution Flow:

- If URL exists:
  - Download favicon.ico
  - Writes to disk (CR433101.dat.exe)
  - Run favicon.ico (CR433101.dat.exe)
- If URL doesn't exist:
  - Delete from disk
  - Do not run