Unkown.Malware.exe File

Hashes

- SHA256--> 92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a *Malware.Unknown.exe.malz
- MD5--> 1d8562c0adcaee734d63f7baaca02f7c *Malware.Unknown.exe.malz

---

Floss

FLOSS static Unicode strings

jjjj

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\CR433101.dat.exe

open

FLOSS decoded 0 strings

FLOSS extracted 2 stackstrings

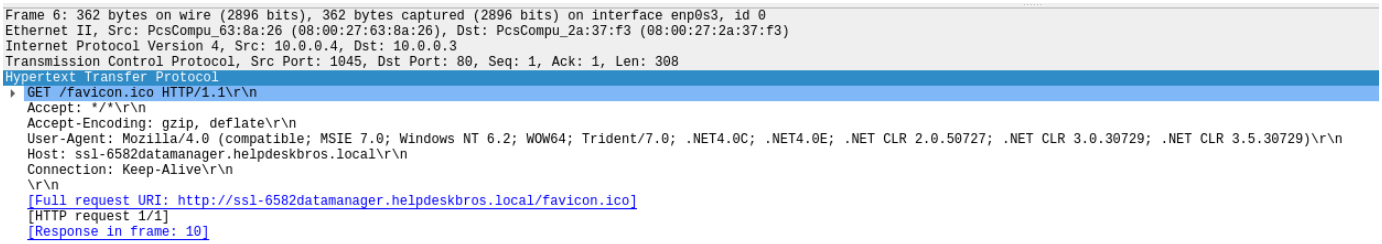
<2_/

ineIGenu

HTTP request by malware

Captured using wireshark

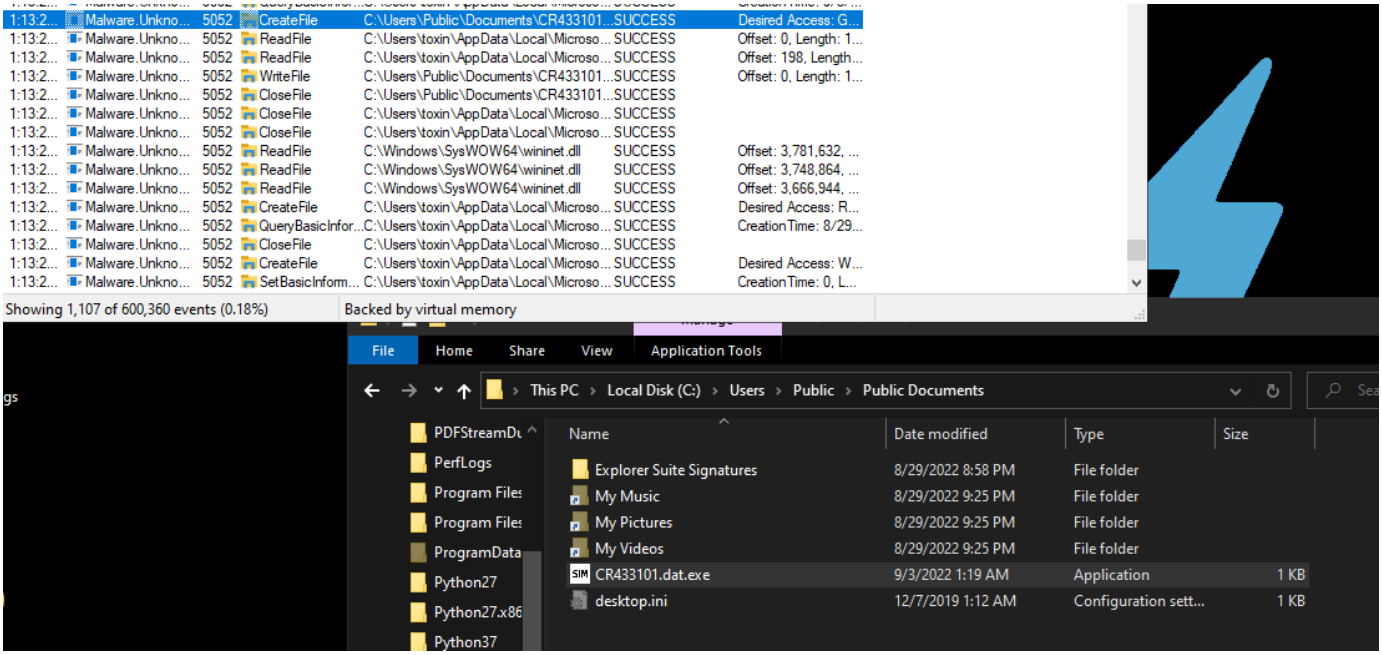
Filter used--->`http.request.full_uri contains favicon.ico`

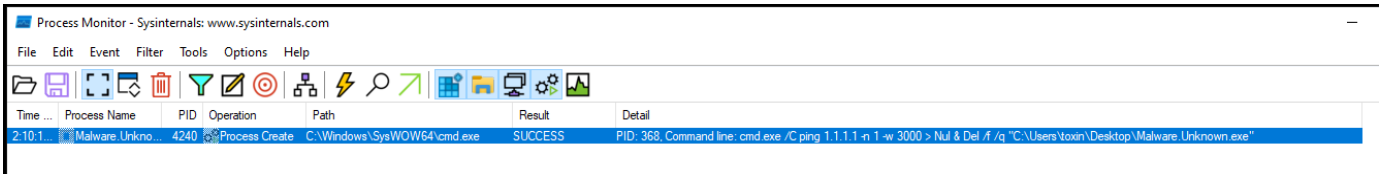


Host Indicators

Created a File as shown in Floss in *C:\Users\Public\Documents\CR433101.dat.exe*

Found using Procmon





URL: http://ssl-6582datamanager.helpdeskbros.local/favicon.ico

Program Execution Flow:

- If URL exists (opens)
  - Download favicon.ico
  - Writes to disk (CR433101.dat.exe)
  - Run favicon.ico (CR433101.dat.exe)
- If URL doesn't exists
  - Stop running exe file
  - Delete the the exe file form the desktop

Conclusion

This malware downloads a dropper form URL using favicon.ico