home.exe

Is DLL ✗ | Packer ✓ | Anti Debug ✗ | Anti VM ✗ | Signed ✗ | XOR ✗

MalFamily: Msilperseus **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	151.00 KB (154624 bytes)
Compile time:	2018-05-02 01:48:03
MD5:	c6dfc506c1d474edb559c9f700fa6d40
SHA1:	0c813ccb6154c902931cfac17faa00874cf29ff6
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-05-07 03:27:02

URL(s) file hosting

http://dhm-mhn.com/ifeoma/home.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-05-06 00:42:37	49/66	

Import library

mscoree.dll

5 Behaviors detected by system signatures

Executed a process and injected code into it, probably while unpacking

- Injection: home.exe(2404) -> None(2540)

Creates RWX memory

Network activity detected but not expressed in API logs

Performs some HTTP requests

- url: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.92, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00024200, virtual_size: 0x00024054

1 HTTP Request(s) detected

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab

Hostname: www.download.windowsupdate.com

IP Address: 93.184.221.240

Port: 80

Count: 1