4.exe

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

MalScore: 100

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	233.50 KB (239104 bytes)
Compile time:	2018-05-07 09:22:53
MD5:	8acb1a113d20530f501fc371622ff0db
SHA1:	3e3996eac73c8c5b100e578bf8794f61fb47d255
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-05-07 18:06:03

URL(s) file hosting

http://panelonetwothree.ml/07/new/xe/4.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-05-07 15:21:37	28/64	

Import library

mscoree.dll

10 Behaviors detected by system signatures

Creates a copy of itself

- copy: C:\Users\Seven01\4.exe

Installs itself for autorun at Windows startup

- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\PkKqJI.url
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\PkKqJI.url

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

- Injection: 4.exe(2388) -> vbc.exe(2868)

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\4.exe:Zone.Identifier

Anomalous .NET characteristics

- anomalous_version: Assembly version is set to 0

The binary likely contains encrypted or compressed data.

- section: name: .rsrc, entropy: 7.76, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_READ, raw_size: 0x00027c00, virtual_size: 0x00027bba

At least one IP Address, Domain, or File Name was found in a crypto call

- ioc: -3.117606E
- ioc: 6.270817E-34F
- ioc: -3.322591
- ioc: -1.068504E
- ioc: 5.841241E-08
- ioc: 7.942857E-38F
- ioc: 2.860554E-17
- ioc: 4.059636E
- ioc: 1.0.0.0
- ioc: pplication.app
- ioc: asm.v2

A process attempted to delay the analysis task.

- Process: vbc.exe tried to sleep 1050 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

Attempts to connect to a dead IP:Port (1 unique times)

- IP: 192.168.56.1:3324