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:	173.50 KB (177664 bytes)
Compile time:	2018-04-02 17:26:05
MD5:	3c7e5080c12f4e9a63d5a770fa57051c
SHA1:	3d098a0606d70094a7be2a05f0c40d169f0497c2
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-04-05 13:45:03

URL(s) file hosting

http://onedrivenet.xyz/work/exe/4.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-04-03 23:04:30	13/66	

Import library

mscoree.dll

11 Behaviors detected by system signatures

Attempts to modify Explorer settings to prevent hidden files from being displayed

Creates a copy of itself

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

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\f249a110be4f465272d1292f10731d3a
- data: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe" ..
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\f249a110be4f465272d1292f10731d3a
- data: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe" ..
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\.url
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\f249a110be4f465272d1292f10731d3a.exe
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\.url
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\f249a110be4f465272d1292f10731d3a.exe

Sniffs keystrokes

- GetAsyncKeyState: Process: RegAsm.exe(2472)

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

- Injection: 4.exe(2072) -> RegAsm.exe(2472)

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

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

- ioc: kernel32.dll
- ioc: 1.0.0.0
- ioc: pplication.app
- ioc: asm.v2

A process attempted to delay the analysis task.

- Process: RegAsm.exe tried to sleep 297 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

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

- IP: 45.35.158.170:2445 (United States)

1 Host(s) detected

IP Address	Hostname	Reverse DNS
45.35.158.170		unassigned.psychz.net.

1 Countr(y|ies) detected

Hosts	Country
1	United States