im6.exe

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

MalFamily: Razy **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	669.88 KB (685952 bytes)
Compile time:	2018-05-19 01:32:16
MD5:	10349a36cbd8aa3a5f13b3a591432218
SHA1:	236083b08295a9ecfbc43f5c603d752f6b9ed868
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-07-17 14:39:04

URL(s) file hosting

http://lnx.hdmiservice.com/im6.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-06-21 13:55:06	47/68	

Import library

mscoree.dll

16 Behaviors detected by system signatures

Collects information to fingerprint the system

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Local\Temp\Windows\svchost.exe

Checks the CPU name from registry, possibly for anti-virtualization

Retrieves Windows ProductID, probably to fingerprint the sandbox

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Local\Temp\Windows

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load
- data: C:\Users\Seven01\AppData\Local\Temp\Windows\svchost.exe.lnk
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\svchost.exe.lnk
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\svchost.exe.lnk

A process attempted to delay the analysis task by a long amount of time.

- Process: WmiPrvSE.exe tried to sleep 601 seconds, actually delayed analysis time by 0 seconds
- Process: svhost.exe tried to sleep 4084 seconds, actually delayed analysis time by 0 seconds

Sniffs keystrokes

- SetWindowsHookExA: Process: svhost.exe(2924)

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Local\Temp\svhost.exe:Zone.Identifier

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

- Injection: im6.exe(2560) -> svhost.exe(2924)

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.85, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00068c00, virtual_size: 0x00068a94

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Local\Temp\svhost.exe

A process created a hidden window

- Process: im6.exe -> "cmd.exe"

Reads data out of its own binary image

- self_read: process: im6.exe, pid: 2560, offset: 0x00000000, length: 0x00001000
- self_read: process: im6.exe, pid: 2560, offset: 0x00000080, length: 0x00000200

Creates RWX memory

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

- IP: 192.168.56.1:3339