p.exe

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

MalFamily: Nanocore **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	1363.50 KB (1396224 bytes)
Compile time:	2018-04-24 18:38:14
MD5:	5d36aa1fea2ce38148c245b93da0e4ae
SHA1:	a4a34aa774828bfa9ce27c22778b832e90a4b5b9
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-04-27 13:57:07

URL(s) file hosting

http://www.medconrx.com/done/p.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-04-27 02:00:55	21/67	

Import library

mscoree.dll

15 Behaviors detected by system signatures

Collects information to fingerprint the system

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\FolderN\name.exe

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Roaming\FolderN

Exhibits behavior characteristic of Nanocore RAT

Installs itself for autorun at Windows startup

- key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\UPNP Subsystem
- data: C:\Program Files (x86)\UPNP Subsystem\upnpss.exe
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load
- data: C:\Users\Seven01\AppData\Roaming\FolderN\name.exe.lnk
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\name.exe.lnk
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\name.exe.lnk

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: p.exe(2388) -> svhost.exe(2820)

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.68, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x0004a600, virtual_size: 0x0004a5a1

Drops a binary and executes it

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

A process created a hidden window

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

Reads data out of its own binary image

- self_read: process: p.exe, pid: 2388, offset: 0x00000000, length: 0x00001000
- self_read: process: p.exe, pid: 2388, offset: 0x00000080, length: 0x00000200
- self_read: process: svhost.exe, pid: 2820, offset: 0x00000000, length: 0x00001000
- self_read: process: svhost.exe, pid: 2820, offset: 0x00000080, length: 0x00000200
- self_read: process: svhost.exe, pid: 2820, offset: 0x00000178, length: 0x00000200
- self_read: process: svhost.exe, pid: 2820, offset: 0x0000f5f4, length: 0x00000200
- self_read: process: svhost.exe, pid: 2820, offset: 0x0000f610, length: 0x00000200

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

- ioc: v2.0.50727

A process attempted to delay the analysis task.

- Process: svhost.exe tried to sleep 545 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

Attempts to connect to a dead IP:Port (2 unique times)

- IP: 192.168.56.1:1002
- IP: 89.35.228.194:1002 (Romania)

3 Host(s) detected

IP Address	Hostname	Reverse DNS
89.35.228.194		i.89.35.228.194.use.teentelecom.net.
8.8.8.8		google-public-dns-a.google.com.
8.8.4.4		google-public-dns-b.google.com.

2 Countr(y|ies) detected

Hosts	Country
2	United States
1	Romania