63.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:	203.00 KB (207872 bytes)
Compile time:	2015-02-22 01:49:37
MD5:	b91ef5418904c2e0ed9f3f0508961520
SHA1:	c3c5e5f26a47f84e6097cd52949394e3332fcccb
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-02-20 13:33:06

URL(s) file hosting

http://guelphupholstery.com/images/yupsia/exe/63.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-02-20 07:39:05	54/68	

Import library

mscoree.dll

13 Behaviors detected by system signatures

Collects information to fingerprint the system

Creates a copy of itself

- copy: C:\Program Files (x86)\UPNP Subsystem\upnpss.exe

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
- file: C:\Windows\Tasks\Adobe Flash Player Updater.job
- file: C:\Windows\Tasks\Adobe Flash Player Updater.job

Attempts to repeatedly call a single API many times in order to delay analysis time

- Spam: services.exe (488) called API GetSystemTimeAsFileTime 3228438 times

The binary likely contains encrypted or compressed data.

- section: name: .rsrc, entropy: 8.00, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_READ, raw_size: 0x00016000, virtual_size: 0x00015f98

Performs some HTTP requests

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

A process created a hidden window

- Process: 63.exe -> "schtasks.exe" /create /f /tn "UPNP Subsystem" /xml "C:\Users\Seven01\AppData\Local\Temp\tmpB12F.tmp"
- Process: 63.exe -> "schtasks.exe" /create /f /tn "UPNP Subsystem Task" /xml "C:\Users\Seven01\AppData\Local\Temp\tmpC0FF.tmp"

Reads data out of its own binary image

- self_read: process: 63.exe, pid: 2412, offset: 0x00000000, length: 0x00001000
- self_read: process: 63.exe, pid: 2412, offset: 0x00000080, length: 0x00000200

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

- ioc: v2.0.50727
- ioc: inetsim.org0

A process attempted to delay the analysis task.

- Process: 63.exe tried to sleep 467 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

Attempts to connect to a dead IP:Port (3 unique times)

- IP: 192.168.56.1:7171
- IP: 192.168.56.1:80
- IP: 192.168.56.1:443

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: 95.101.180.128

Port: 80
Count: 1