sk.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:	733.50 KB (751104 bytes)
Compile time:	2017-11-13 10:10:22
MD5:	76e280921dafc3cf1bcc4bf354cef369
SHA1:	5b0c3071aa63e18aa91af59083223d3cceb0fa3c
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2017-11-20 11:36:52

URL(s) file hosting

http://ssrdevelopments.co.za/tt/sk.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2017-11-20 10:43:39	12/67	

Import library

mscoree.dll

15 Behaviors detected by system signatures

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\Skype.exe

- copy: C:\Users\Seven01\AppData\Roaming\TcPR.exe
- copy: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\b8d41a36c0f1de1ae26bf020f0fd54bc.exe

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Roaming\Skype.exe
- file: C:\Users\Seven01\AppData\Roaming\TcPR.exe

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\b8d41a36c0f1de1ae26bf020f0fd54bc
- data: "C:\Users\Seven01\AppData\Roaming\TcPR.exe" ..
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\b8d41a36c0f1de1ae26bf020f0fd54bc
- data: "C:\Users\Seven01\AppData\Roaming\TcPR.exe" ..
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\b8d41a36c0f1de1ae26bf020f0fd54bc.exe
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\b8d41a36c0f1de1ae26bf020f0fd54bc.exe
- file: C:\Windows\Tasks\Adobe Flash Player Updater.job
- file: C:\Windows\Tasks\Adobe Flash Player Updater.job

A process was set to shut the system down when terminated

- process: TcPR.exe:2596

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

- Spam: services.exe (484) called API GetSystemTimeAsFileTime 1799453 times

Sniffs keystrokes

- GetAsyncKeyState: Process: TcPR.exe(2596)

The binary likely contains encrypted or compressed data.

- section: name: Oo-PmoFB, entropy: 7.94, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ|IMAGE_SCN_MEM_WRITE, raw_size: 0x00000c00, virtual_size: 0x00000a3c
- section: name: .text, entropy: 7.99, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x000a5400, virtual_size: 0x000a5308

Performs some HTTP requests

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

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Roaming\TcPR.exe
- binary: C:\Users\Seven01\AppData\Roaming\Skype.exe

A process created a hidden window

- Process: sk.exe -> "cmd"
- Process: Skype.exe -> "cmd"
- Process: Skype.exe -> "cmd"
- Process: Skype.exe -> "cmd"
- Process: Skype.exe -> "cmd"
- Process: Skype.exe -> "cmd"
- Process: Skype.exe -> "cmd"
- Process: TcPR.exe -> "cmd"

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

Reads data out of its own binary image

- self_read: process: Skype.exe, pid: 2776, offset: 0x00000000, length: 0x000b7600

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

- ioc: inetsim.org0

A process attempted to delay the analysis task.

- Process: TcPR.exe tried to sleep 786 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

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

- IP: 192.168.56.1:80
- IP: 192.168.56.1:443
- IP: 212.83.167.116:1604 (France)

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: 2.228.46.122

Port: 80

Count: 1

1 Host(s) detected

IP Address	Hostname	Reverse DNS
212.83.167.116		212-83-167-116.rev.poneytelecom.eu.

1 Countr(y|ies) detected

Hosts	Country
1	France