9.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:	818.00 KB (837632 bytes)
Compile time:	2018-04-29 19:11:30
MD5:	b2c6201fbf33abdaacb838ad410ecab8
SHA1:	beb9a1b44f7e687ecd1e6728519b315223e46d1c
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-04-30 19:27:03

URL(s) file hosting

http://stevemike-fireforce.info/work/newexe/9.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-04-30 06:50:13	31/67	↗

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\filename.exe

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

Retrieves Windows ProductID, probably to fingerprint the sandbox

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Update
- data: cmd /c type C:\Users\Seven01\AppData\Local\Temp\Update.txt | cmd

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

- Process: WmiPrvSE.exe tried to sleep 661 seconds, actually delayed analysis time by 0 seconds
- Process: filename.exe tried to sleep 4343 seconds, actually delayed analysis time by 0 seconds

Sniffs keystrokes

- SetWindowsHookExA: Process: filename.exe(2976)

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Roaming\filename.exe:Zone.Identifier

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

- Injection: filename.exe(2728) -> filename.exe(2976)

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.99, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00071a00, virtual_size: 0x00071884

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\filename.exe

A process created a hidden window

- Process: 9.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"
- Process: filename.exe -> "cmd"

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

Creates RWX memory

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

- IP: 192.168.56.1:9028

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: 95.101.180.88

Port: 80

Count: 1