p1.exe

Is DLL ⊗ | **Packer ✔** | Anti Debug ⊗ | Anti VM ⊗ | Signed ⊗ | XOR ⊗

MalFamily: Darkcomet **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	1136.00 KB (1163264 bytes)
Compile time:	2018-04-26 18:54:38
MD5:	b2aa6bd41f3a8b4a0aef513189ca4fd6
SHA1:	b46851e8a68516553279cec65aa05619e42c6cd8
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-04-27 13:54:06

URL(s) file hosting

http://www.medconrx.com/done/p1.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-04-27 02:44:14	11/67	↗

Import library

mscoree.dll

13 Behaviors detected by system signatures

Creates known Fynloski/DarkComet mutexes

Interacts with known DarkComet registry keys

- Key: HKEY_CURRENT_USER\Software\DC3_FEXEC
- Key: HKEY_CURRENT_USER\Software\DC3_FEXEC\{846ee340-7039-11de-9d20-806e6f6e6963-3837576413}
- Key: HKEY_CURRENT_USER\Software\DC2_USERS

Creates a copy of itself

- copy: C:\Users\Seven01\Documents\MSDCSC\msdcsc.exe

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Local\Temp\p1.exe
- file: C:\Users\Seven01\Documents\MSDCSC\msdcsc.exe

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\MicroUpdate
- data: C:\Users\Seven01\Documents\MSDCSC\msdcsc.exe
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Update
- data: cmd /c type C:\Users\Seven01\AppData\Local\Temp\Update.txt | cmd
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\UserInit
- data: C:\Windows\system32\userinit.exe,C:\Users\Seven01\Documents\MSDCSC\msdcsc.exe

Sniffs keystrokes

- SetWindowsHookExA: Process: msdcsc.exe(2704)

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

- Injection: p1.exe(2532) -> p1.exe(2856)

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 8.00, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00117c00, virtual_size: 0x00117be4

Drops a binary and executes it

- binary: C:\Users\Seven01\Documents\MSDCSC\msdcsc.exe

A process created a hidden window

- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"

- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: p1.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> "cmd"
- Process: msdcsc.exe -> notepad

A process attempted to delay the analysis task.

- Process: p1.exe tried to sleep 427 seconds, actually delayed analysis time by 0 seconds
- Process: msdcsc.exe tried to sleep 520 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

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

- IP: 192.168.56.1:1604