minerupdate.exe

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

MalFamily: Ispy **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	1829.84 KB (1873760 bytes)
Compile time:	2018-05-28 00:24:26
MD5:	4fa1915159ca5d200a5d9c946ccf0bb3
SHA1:	f80cc2978efcdfc0d03a749effe755c0b64a872c
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-05-27 19:27:09

URL(s) file hosting

http://www.apl.com.pk/loc/php/minerupdate.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-05-27 15:54:43	21/66	

Import library

mscoree.dll

15 Behaviors detected by system signatures

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\Microsoft\mcm.exe

Creates a hidden or system file

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

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load
- data: C:\Users\Seven01\AppData\Roaming\Microsoft\mcm.exe.lnk

Exhibits behavior characteristic of iSpy Keylogger

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\ProgramData\eUbHLgwTSi\ggkanor2.exe:Zone.Identifier

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

- Injection: minerupdate.exe(2432) -> svhost.exe(2764)

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.92, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x0017c600, virtual_size: 0x0017c5b4

Drops a binary and executes it

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

A process created a hidden window

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

Reads data out of its own binary image

- self_read: process: minerupdate.exe, pid: 2432, offset: 0x00000000, length: 0x00001000
- self_read: process: minerupdate.exe, pid: 2432, offset: 0x00000080, length: 0x00000200
- self_read: process: svhost.exe, pid: 2764, offset: 0x00000000, length: 0x00001000
- self_read: process: svhost.exe, pid: 2764, offset: 0x00000080, length: 0x00000200
- self_read: process: svhost.exe, pid: 2764, offset: 0x00000178, length: 0x00000200
- self_read: process: svhost.exe, pid: 2764, offset: 0x0000f5f4, length: 0x00000200
- self_read: process: svhost.exe, pid: 2764, offset: 0x0000f610, length: 0x00000200
- self_read: process: svhost.exe, pid: 2972, offset: 0x00000000, length: 0x00001000
- self_read: process: svhost.exe, pid: 2972, offset: 0x00000080, length: 0x00000200
- self_read: process: svhost.exe, pid: 2972, offset: 0x00000178, length: 0x00000200
- self_read: process: svhost.exe, pid: 2972, offset: 0x0000f5f4, length: 0x00000200
- self_read: process: svhost.exe, pid: 2972, offset: 0x0000f610, length: 0x00000200
- self_read: process: svhost.exe, pid: 2088, offset: 0x00000000, length: 0x00001000
- self_read: process: svhost.exe, pid: 2088, offset: 0x00000080, length: 0x00000200
- self_read: process: svhost.exe, pid: 2088, offset: 0x00000178, length: 0x00000200
- self_read: process: svhost.exe, pid: 2088, offset: 0x0000f5f4, length: 0x00000200
- self_read: process: svhost.exe, pid: 2088, offset: 0x0000f610, length: 0x00000200

Repeatedly searches for a not-found process, may want to run with startbrowser=1 option

Network anomalies occured during the analysis.

- Anomaly: '144.208.127.27' getaddrinfo with no actual connection to the IP.

A process attempted to delay the analysis task.

- Process: svhost.exe tried to sleep 388 seconds, actually delayed analysis time by 0 seconds
- Process: WmiPrvSE.exe tried to sleep 360 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

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

- IP: 144.208.127.27:3333 (United States)

1 Host(s) detected

IP Address	Hostname	Reverse DNS
144.208.127.27		

1 Countr(y|ies) detected

Hosts	Country
1	United States