khalifer.exe

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

MalFamily: Malicious **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	606.50 KB (621056 bytes)
Compile time:	2017-05-08 05:01:26
MD5:	cbc07da2b936772cb8ea4bc06283e307
SHA1:	4be0e2425b8ebbec79ce416196a06a81ae602a03
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-02-15 11:33:03

URL(s) file hosting

http://prosciuttiamo.it/ice/khalifer.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-02-15 08:30:09	17/63	

Import library

mscoree.dll

9 Behaviors detected by system signatures

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Local\Temp\khalifer.exe:Zone.Identifier

Crashed cuckoomon during analysis. Report this error to the Github repo.

 - pid: 2568
 - message: Exception reported at offset 0x12410 in cuckoomon itself while accessing 0x40 from hook RtlDispatchException

Installs itself for autorun at Windows startup

 - key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\index
 - data: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Templates\index.exe -boot

Creates a copy of itself

 - copy: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Templates\index.exe

Anomalous binary characteristics

 - anomaly: Unprintable characters found in section name

Creates RWX memory

A process created a hidden window

 - Process: index.exe -> C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Templates\index.exe

Drops a binary and executes it

 - binary: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Templates\index.exe

The binary likely contains encrypted or compressed data.

 - section: name: \x08\x11\x02\x18MW!\x05, entropy: 8.00, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ|IMAGE_SCN_MEM_WRITE, raw_size: 0x0000da00, virtual_size: 0x0000d948
 - section: name: .text, entropy: 7.93, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00055c00, virtual_size: 0x00055bd0