TT%20Copy.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:	200.00 KB (204800 bytes)
Compile time:	2017-07-07 06:57:56
MD5:	1b97e84fd02c685f4903831284119443
SHA1:	f7ab4304ae5bc5e1f65d85163d3140d39219a669
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2017-07-14 13:36:03

URL(s) file hosting

http://gulfseoagency.com/new/hn/TT%20Copy.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2017-07-14 10:59:50	42/62	

Import library

mscoree.dll

14 Behaviors detected by system signatures

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\TT Copy

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Local\Temp\TT20Copy.exe

Installs itself for autorun at Windows startup

- file: C:\Windows\Tasks\Adobe Flash Player Updater.job

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

- Spam: services.exe (484) called API GetSystemTimeAsFileTime 1259993 times

Queries information on disks, possibly for anti-virtualization

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

- Injection: TT20Copy.exe(2108) -> TT20Copy.exe(2896)

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.56, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x0002f000, virtual_size: 0x0002ec24

Performs some HTTP requests

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

A process created a hidden window

- Process: TT20Copy.exe -> schtasks.exe

Reads data out of its own binary image

- self_read: process: TT20Copy.exe, pid: 2108, offset: 0x00000000, length: 0x00032000

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: sppsvc.exe tried to sleep 300 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

Attempts to connect to a dead IP:Port (2 unique times)

- IP: 192.168.56.1:443
- IP: 192.168.56.1:80

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: 2.228.46.112
Port: 80
Count: 1