# 24.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:** | 319.50 KB (327168 bytes) |
| **Compile time:** | 2018-04-25 07:30:19 |
| **MD5:** | b78cf1a172ab553e54a45a3446f909c6 |
| **SHA1:** | ceb9d1aaf34673d5a21261d34bf5046d230f391e |
| **Import hash:** | f34d5f2d4577ed6d9ceec516c1f5a744 |
| **Submitted:** | 2018-04-25 17:39:05 |

### URL(s) file hosting

http://panelonetwothree.ml/simon/exp/xe/24.exe

### Antivirus Report

| Report date | Detection Ratio | Permalink |
|---|---|---|
| 2018-04-25 07:59:39 | 15/67 |  |

### Import library

mscoree.dll

## 10 Behaviors detected by system signatures

Creates a copy of itself

- copy: C:\Users\Seven01\24.exe

Installs itself for autorun at Windows startup

- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\mefCUp.url
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\mefCUp.url

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

- Injection: 24.exe(2388) -> vbc.exe(2844)

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\24.exe:Zone.Identifier

Anomalous .NET characteristics

- anomalous_version: Assembly version is set to 0

The binary likely contains encrypted or compressed data.

- section: name: .rsrc, entropy: 7.97, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_READ, raw_size: 0x00024c00, virtual_size: 0x00024b22

At least one IP Address, Domain, or File Name was found in a crypto call

- ioc: 1.406668E-38F
- ioc: 8.858294E-32
- ioc: -4.131418E
- ioc: -4.722018E-06F
- ioc: -3.70759E
- ioc: 3.103807E-21F
- ioc: 3.648264E-28
- ioc: 5.838335E-33
- ioc: -8.672725E
- ioc: 1.0.0.0
- ioc: pplication.app
- ioc: asm.v2

A process attempted to delay the analysis task.

- Process: vbc.exe tried to sleep 1050 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

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

- IP: 192.168.56.1:3324