# boboprotect.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:** | 315.00 KB (322560 bytes) |
| **Compile time:** | 2017-07-12 04:00:29 |
| **MD5:** | 8238276ce326793b492b5bfcf02102c9 |
| **SHA1:** | 1450ccbd8698d51810c4b14003ddd02578e4aecc |
| **Import hash:** | f34d5f2d4577ed6d9ceec516c1f5a744 |
| **Submitted:** | 2017-07-14 13:42:02 |

### URL(s) file hosting

http://gulfseoagency.com/new/hn/boboprotect.exe

### Antivirus Report

| Report date | Detection Ratio | Permalink |
|---|---|---|
| 2017-07-14 09:27:15 | 16/63 | |

### Import library

mscoree.dll

## 5 Behaviors detected by system signatures

Deletes its original binary from disk

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

- Injection: xcas.exe(2328) -> xcas.exe(2440)

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\xcesd
- data: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\xcas.exe
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\xcesd
- data: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\xcas.exe
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\xcas.exe

Creates RWX memory

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.48, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00048a00, virtual_size: 0x00048824