# build.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:** | 909.50 KB (931328 bytes) |
| **Compile time:** | 2018-03-22 16:02:30 |
| **MD5:** | 0766f3d3a085ff223182010af4678eef |
| **SHA1:** | 3b4c8be4d002121a9e604864fbe1897c598467c0 |
| **Import hash:** | f34d5f2d4577ed6d9ceec516c1f5a744 |
| **Submitted:** | 2018-04-14 20:12:02 |

### URL(s) file hosting

http://vigovrus84.had.su/build.exe

### Antivirus Report

| Report date | Detection Ratio | Permalink |
|---|---|---|
| 2018-04-14 02:01:00 | 53/67 | |

### Import library

mscoree.dll

## 14 Behaviors detected by system signatures

Attempts to modify or disable Security Center warnings

Creates a copy of itself

- copy: C:\Program Files\Orcus\Orcus.exe

Creates a hidden or system file

- file: C:\Program Files\Orcus\Orcus.exe

Installs itself for autorun at Windows startup

- service name: WindowsInput
- service path: "C:\Windows\SysWOW64\WindowsInput.exe"
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Orcus
- data: "C:\Program Files\Orcus\Orcus.exe"

Exhibits behavior characteristic of iSpy Keylogger

- C2: 185.209.23.119

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

- Spam: services.exe (488) called API GetSystemTimeAsFileTime 1779786 times
- Spam: WindowsInput.exe (2880) called API NtCreateNamedPipeFile 32872 times

Queries information on disks, possibly for anti-virtualization

Sniffs keystrokes

- SetWindowsHookExA: Process: Orcus.exe(3028)

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.16, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x000e2a00, virtual_size: 0x000e2944

Drops a binary and executes it

- binary: C:\Program Files\Orcus\Orcus.exe
- binary: C:\Windows\SysWOW64\WindowsInput.exe

A process attempted to delay the analysis task.

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

Creates RWX memory

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

- IP: 185.209.23.119:10134 (unknown)

At least one process apparently crashed during execution

## 1 Host(s) detected

| IP Address | Hostname | Reverse DNS |
|---|---|---|
| 185.209.23.119 | | vigrus.club. |

## 1 Countr(y|ies) detected

| Hosts | Country |
|---|---|
| 1 | unknown  |