# qury.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:** | 274.50 KB (281088 bytes) |
| **Compile time:** | 2018-06-20 23:54:35 |
| **MD5:** | 0dbf58d174e22519f799125bfebac6f4 |
| **SHA1:** | 894bfb6da76db8696451ebc8aecff101f6f0d3e9 |
| **Import hash:** | f34d5f2d4577ed6d9ceec516c1f5a744 |
| **Submitted:** | 2018-06-21 22:51:05 |

### URL(s) file hosting

http://rvaginfra.com/include/qury.exe

### Antivirus Report

| Report date | Detection Ratio | Permalink |
|---|---|---|
| 2018-06-21 07:14:21 | 23/69 | |

### Import library

mscoree.dll

## 7 Behaviors detected by system signatures

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

- Injection: qury.exe(2468) -> vbc.exe(2864)

Creates RWX memory

A process attempted to delay the analysis task.

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

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

- ioc: kernel32.dll
- ioc: 1.0.0.0
- ioc: pplication.app
- ioc: asm.v2

The binary likely contains encrypted or compressed data.

- section: name: .rsrc, entropy: 7.98, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_READ, raw_size: 0x00024400, virtual_size: 0x00024212

Anomalous .NET characteristics

- anomalous_version: Assembly version is set to 0

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

- IP: 185.208.211.61:3360 (unknown)

## 1 Host(s) detected

| IP Address | Hostname | Reverse DNS |
|---|---|---|
| 185.208.211.61 ? | | |

## 1 Countr(y|ies) detected

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