# tyuvsn.exe

Is DLL ✗ | Packer ✓ | Anti Debug ✗ | Anti VM ✗ | Signed ✓ | XOR ✗

**MalFamily: Barys** **MalScore: 100**

| | |
|---|---|
| **File type:** | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| **File size:** | 1036.56 KB (1061440 bytes) |
| **Compile time:** | 2017-11-08 15:55:45 |
| **MD5:** | 5029198b44fb643abc3cc2eb61694559 |
| **SHA1:** | 8d9448fe66203dd72c8780a4fffd845691a02ed6 |
| **Import hash:** | f34d5f2d4577ed6d9ceec516c1f5a744 |
| **Submitted:** | 2017-11-19 19:36:03 |

### URL(s) file hosting

http://ronqpeng.com/new/tyuvsn.exe

### Antivirus Report

| Report date | Detection Ratio | Permalink |
|---|---|---|
| 2017-11-19 11:56:30 | 32/67 |  |

### Import library

mscoree.dll

## 13 Behaviors detected by system signatures

Creates a copy of itself

- copy: C:\Windows\System32\svchosts.exe

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Local\Temp\.Identifier
- file: C:\Windows\SysWOW64\.Identifier

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Update
- data: cmd /c type C:\Users\Seven01\AppData\Local\Temp\Update.txt | cmd

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

- Injection: svchosts.exe(1344) -> svchosts.exe(1872)

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.98, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x0004ee00, virtual_size: 0x0004ec34
- section: name: .rsrc, entropy: 8.00, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_READ, raw_size: 0x000b2800, virtual_size: 0x000b2800

Performs some HTTP requests

- url: http://s2.symcb.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBS56bKHAoUD%2BOyl%2B0LhPg9JxyQm4gQUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMCED141%2Fl2SWCyYX308B7Khio%3D
- url: http://s2.symcb.com/
- url: http://s1.symcb.com/pca3-g5.crl
- url: http://sv.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQe6LNDJdqx%2BJOp7hVgTeaGFJ%2FCQgQUljtT8HkzI699g%2B8uK8zKt4YecmYCEBLwJ34PIzs5%2BUGbBujN41I%3D
- url: http://sv.symcd.com/
- url: http://sv.symcb.com/sv.crl

HTTP traffic contains suspicious features which may be indicative of malware related traffic

- post_no_referer: HTTP traffic contains a POST request with no referer header
- suspicious_request: http://s2.symcb.com/
- suspicious_request: http://s1.symcb.com/pca3-g5.crl
- suspicious_request: http://sv.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQe6LNDJdqx%2BJOp7hVgTeaGFJ%2FCQgQUljtT8HkzI699g%2B8uK8zKt4YecmYCEBLwJ34PIzs5%2BUGbBujN41I%3D
- suspicious_request: http://sv.symcd.com/
- suspicious_request: http://sv.symcb.com/sv.crl

Drops a binary and executes it

- binary: C:\Windows\SysWOW64\Host.exe
- binary: C:\Users\Seven01\AppData\Local\Temp\Host.exe

A process created a hidden window

- Process: tyuvsn.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"

- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"
- Process: svchosts.exe -> "cmd"

A process attempted to delay the analysis task.

- Process: Host.exe tried to sleep 1950 seconds, actually delayed analysis time by 0 seconds
- Process: svchosts.exe tried to sleep 1362 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

Presents an Authenticode digital signature

- md5_fingerprint: 7f2e08a290c8767afafafffe09be1149
- sha1_fingerprint: 3b75816d15a6d8f4598e9cf5603f1839ee84d73d
- cn: Oracle America, Inc.
- sn: 251730561715847307956233137388035694 90

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

- IP: 212.7.208.88:3360 (Netherlands)
- IP: 192.168.56.1:80

## 6 HTTP Request(s) detected

**http://s2.symcb.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBS56bKHAoUD%2BOyl%2B0LhPg9JxyQm4gQUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMCED141%2Fl2SWCyYX308B7Khio%3D**

Hostname: s2.symcb.com

IP Address: 23.50.155.27

Port: 80

Count: 3

| http://s2.symcb.com/ |
|---|
| Hostname: s2.symcb.com |
| IP Address: 23.50.155.27 |
| Port: 80 |
| Count: 3 |

| http://s1.symcb.com/pca3-g5.crl |
|---|
| Hostname: s1.symcb.com |
| IP Address: 23.50.149.163 |
| Port: 80 |
| Count: 3 |

| http://sv.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQe6LNDJdqx%2BJOp7hVgTeaGFJ%2FCQgQUljtT8Hkzl699g%2B8uK8zKt4YecmYCEBLwJ34PIzs5%2BUGbBujN41I%3D |
|---|
| Hostname: sv.symcd.com |
| IP Address: 23.50.155.27 |
| Port: 80 |
| Count: 3 |

| http://sv.symcd.com/ |
|---|
| Hostname: sv.symcd.com |
| IP Address: 23.50.155.27 |
| Port: 80 |
| Count: 3 |

| http://sv.symcb.com/sv.crl |
|---|
| Hostname: sv.symcb.com |
| IP Address: 23.50.149.163 |
| Port: 80 |
| Count: 3 |

## 1 Host(s) detected

| IP Address | Hostname | Reverse DNS |
|---|---|---|
| 212.7.208.88 | | |

## 1 Countr(y|ies) detected

| Hosts | Country |
|---|---|
| 1 | Netherlands  |