ORDER.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:	260.00 KB (266240 bytes)
Compile time:	2018-05-02 14:06:37
MD5:	d9edbfddad6c8e3614651445203bcb48
SHA1:	3aac073da40b452dca961640fb19c18d8b6bcd44
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-05-03 16:33:06

URL(s) file hosting

http://23.249.161.153/ORDER.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-05-03 04:34:42	25/67	

Import library

mscoree.dll

8 Behaviors detected by system signatures

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

- Injection: ORDER.exe(2384) -> vbc.exe(2872)

Sniffs keystrokes

- SetWindowsHookExA: Process: vbc.exe(2872)

Creates RWX memory

A process attempted to delay the analysis task.

- Process: vbc.exe tried to sleep 420 seconds, actually delayed analysis time by 0 seconds

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

- ioc: 7.183919E
- ioc: 5.362493E-18
- ioc: 198.6944F
- ioc: -5.89698E-18F
- ioc: -2.62394E
- ioc: -1.91406E-17F
- ioc: 1.0.0.0
- ioc: pplication.app
- ioc: asm.v2

The binary likely contains encrypted or compressed data.

- section: name: .rsrc, entropy: 7.67, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_READ, raw_size: 0x00021a00, virtual_size: 0x00021956

Anomalous .NET characteristics

- anomalous_version: Assembly version is set to 0

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

- IP: 192.168.56.1:1690