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:	1620.50 KB (1659392 bytes)
Compile time:	1970-01-01 01:00:00
MD5:	7feccbef4ed3a323ed763d24d022e4df
SHA1:	c6d62240ffd19c94a5f5080d7518b65555eb4fb2
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2017-09-20 18:51:02

URL(s) file hosting

http://ehtbmaroc.com/order.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2017-09-20 15:27:14	27/65	

Import library

mscoree.dll

7 Behaviors detected by system signatures

Creates RWX memory

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

- ioc: inetsim.org0

Reads data out of its own binary image

- self_read: process: order.exe, pid: 2476, offset: 0x00000000, length: 0x00001000
- self_read: process: order.exe, pid: 2476, offset: 0x00000080, length: 0x00000200

Performs some HTTP requests

- url: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab

.NET file is packed/obfuscated with Confuser

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.55, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00194a00, virtual_size: 0x001949a4

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

- IP: 192.168.56.1:80

1 HTTP Request(s) detected

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
Hostname: www.download.windowsupdate.com
IP Address: 95.101.180.138
Port: 80
Count: 1