test8.exe

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

MalFamily: Malicious **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	171.50 KB (175616 bytes)
Compile time:	2018-03-21 01:51:28
MD5:	1b77111c6f6f4a18ce4815e569e6ea2e
SHA1:	1487e52588fa0a041edfc4e7e57b59ce141747ec
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-03-26 23:30:03

URL(s) file hosting

http://www.uwaoma.info/test8.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-03-21 09:53:57	9/64	

Import library

mscoree.dll

6 Behaviors detected by system signatures

Checks the system manufacturer, likely for anti-virtualization

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: test8.exe, pid: 2472, offset: 0x00000000, length: 0x00001000
- self_read: process: test8.exe, pid: 2472, offset: 0x00000080, length: 0x00000200

Performs some HTTP requests

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

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: 93.184.221.240
Port: 80
Count: 1