tydanj.exe

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

MalFamily: GoIroted **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	801.41 KB (820648 bytes)
Compile time:	2017-01-21 13:04:37
MD5:	46078a92c76ea26b8282dbfffbfb6f50
SHA1:	238d7d2f6077a1ccc73cba7b12be37d478eab802
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2017-01-23 19:09:03

URL(s) file hosting

http://149.56.65.124/~jahalele/abj/tydanj.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2017-01-23 16:11:18	12/56	

Import library

mscoree.dll

7 Behaviors detected by system signatures

Attempts to create or modify system certificates

Creates RWX memory

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

- ioc: www.engyn.com1
- ioc: engyn.com0
- ioc: www.digicert.com1
- ioc: http://www.digicert.com/ssl-cps-repository.htm0
- ioc: http://ocsp.digicert.com0C
- ioc: http://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt0
- ioc: http://crl3.digicert.com/DigiCertAssuredIDRootCA.crl0
- ioc: http://crl4.digicert.com/DigiCertAssuredIDRootCA.crl0
- ioc: https://www.digicert.com/CPS0
- ioc: http://crl3.digicert.com/DigiCertAssuredIDCA-1.crl08
- ioc: http://crl4.digicert.com/DigiCertAssuredIDCA-1.crl0w
- ioc: http://ocsp.digicert.com0A
- ioc: http://cacerts.digicert.com/DigiCertAssuredIDCA-1.crt

Performs some HTTP requests

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

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.81, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x000c4000, virtual_size: 0x000c3594

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

- IP: 192.168.56.1:80

Presents an Authenticode digital signature

- md5_fingerprint: c5931ad84bc99651c5dc0ec8f4d83013
- cn: www.engyn.com/emailAddress=ajosh@engyn.com
- sha1_fingerprint: 6059332de6a1fb1c3a95bdd60a16ec93581b8a61
- sn: 12259451678859885702

4 HTTP Request(s) detected

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
Hostname: www.download.windowsupdate.com
IP Address: 95.101.180.113
Port: 80
Count: 3

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
Hostname: www.download.windowsupdate.com
IP Address: 95.101.180.113
Port: 80

Count: 1

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
Hostname: www.download.windowsupdate.com
IP Address: 95.101.180.113
Port: 80
Count: 1

http://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt
Hostname: cacerts.digicert.com
IP Address: 93.184.220.29
Port: 80
Count: 1