HOLLYWOOD.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:	191.15 KB (195736 bytes)
Compile time:	2017-06-09 10:21:52
MD5:	b4a63d13eee189a5920f7a4802f812c7
SHA1:	c410f5effc4eac8afd4c1cf88b1c87a659128d5d
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-03-19 15:21:03

URL(s) file hosting

http://claymorebg.com/HOLLYWOOD.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-03-19 13:19:40	14/65	

Import library

mscoree.dll

4 Behaviors detected by system signatures

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://ocsp.verisign.com/
- suspicious_request: http://crl.verisign.com/pca3-g5.crl
- suspicious_request: http://sf.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTSqZMG5M8TA9rdzkbCnNwuMAd5VgQUz5mp6nsm9EvJjo%2FX8AUm7%2BPSp50CEH7A2sOa42RrFJMnf3YaDsM%3D
- suspicious_request: http://sf.symcd.com/
- suspicious_request: http://sf.symcb.com/sf.crl

Performs some HTTP requests

- url: http://ocsp.verisign.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBS56bKHAoUD%2BOyl%2B0LhPg9JxyQm4gQUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMCEFIA5aolVvwahu2WydRLM8c%3D
- url: http://ocsp.verisign.com/
- url: http://crl.verisign.com/pca3-g5.crl
- url: http://sf.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTSqZMG5M8TA9rdzkbCnNwuMAd5VgQUz5mp6nsm9EvJjo%2FX8AUm7%2BPSp50CEH7A2sOa42RrFJMnf3YaDsM%3D
- url: http://sf.symcd.com/
- url: http://sf.symcb.com/sf.crl

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.71, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x0002bc00, virtual_size: 0x0002baf4

Presents an Authenticode digital signature

- md5_fingerprint: eafb2f22204672f3df5a0aa4f6c8b7d7
- sha1_fingerprint: 2a94c3ea8325934e8a9c3284302cc966244c59b5
- cn: TeamViewer GmbH
- sn: 168484085528458965121727932520833093315

6 HTTP Request(s) detected

http://ocsp.verisign.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBS56bKHAoUD%2BOyl%2B0LhPg9JxyQm4gQUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMCEFIA5aolVvwahu2WydRLM8c%3D

Hostname: ocsp.verisign.com

IP Address: 23.37.43.27

Port: 80

Count: 2

http://ocsp.verisign.com/

Hostname: ocsp.verisign.com

IP Address: 23.37.43.27

Port: 80

Count: 2

http://crl.verisign.com/pca3-g5.crl

Hostname: crl.verisign.com

IP Address: 23.37.37.163
Port: 80
Count: 2

http://sf.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTSqZMG5M8TA9rdzkbCnNwuMAd5VgQUz5mp6nsm9EvJjo%2FX8AUm7%2BPSp50CEH7A2sOa42RrFJMnf3YaDsM%3D
Hostname: sf.symcd.com
IP Address: 23.37.43.27
Port: 80
Count: 2

http://sf.symcd.com/
Hostname: sf.symcd.com
IP Address: 23.37.43.27
Port: 80
Count: 2

http://sf.symcb.com/sf.crl
Hostname: sf.symcb.com
IP Address: 23.37.37.163
Port: 80
Count: 2