fis.exe

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

MalFamily: Ursu **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	806.05 KB (825400 bytes)
Compile time:	2017-08-11 12:40:03
MD5:	c6650e415309c2b196aa486735dad543
SHA1:	5312a32fcf53b83a6a329b8b70320dddb4fe6fe0
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-05-22 22:57:07

URL(s) file hosting

http://notificetionwem.fr.nf/sas/fis.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-05-22 02:30:25	23/66	

Import library

mscoree.dll

3 Behaviors detected by system signatures

Performs some HTTP requests

- url:

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

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.97, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x000b5400, virtual_size: 0x000b5374

Presents an Authenticode digital signature

- md5_fingerprint: 78989302406896b6dc127192d368f10d
- sha1_fingerprint: 4022bb3c0398d595623a5380d5eeb520fc6150aa
- cn: Simon Tatham
- sn: 144649655500629036263424739845518494587

3 HTTP Request(s) detected

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
Hostname: www.download.windowsupdate.com
IP Address: 13.107.4.50
Port: 80
Count: 5

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
Hostname: www.download.windowsupdate.com
IP Address: 13.107.4.50
Port: 80
Count: 1

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
Hostname: www.download.windowsupdate.com
IP Address: 13.107.4.50
Port: 80
Count: 5