fred.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:	288.00 KB (294912 bytes)
Compile time:	2018-07-05 20:54:33
MD5:	77031e1f87a144b9138dc68d65dac9f7
SHA1:	8c1495c11cb82b9fe3091ffaf32ec7ac53947185
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-07-10 11:36:04

URL(s) file hosting

http://cofancio.com/fred.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-07-09 18:17:13	47/66	

Import library

mscoree.dll

3 Behaviors detected by system signatures

Executed a process and injected code into it, probably while unpacking

- Injection: fred.exe(2460) -> None(2624)

Creates RWX memory

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.98, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00035000, virtual_size: 0x00034e04