imgclone.exe

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

MalFamily: Razy **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	803.00 KB (822272 bytes)
Compile time:	2018-05-28 15:34:05
MD5:	5430c25a993989a9489ed62a311e2f81
SHA1:	66a3f0554eeff2e5accab3107b5c6bfff16bced9
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-05-29 20:33:13

URL(s) file hosting

http://urganchsh28-m.uz//wp-content/imgclone.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-05-29 17:04:32	27/66	

Import library

mscoree.dll

3 Behaviors detected by system signatures

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: 0x00020400, virtual_size: 0x00020284
- section: name: .rsrc, entropy: 7.99, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_READ, raw_size: 0x000a8400, virtual_size: 0x000a82d8

Anomalous .NET characteristics

- anomalous_version: Assembly version is set to 0