scan%20copy84756786545.exe

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

MalFamily: Barys **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	511.00 KB (523264 bytes)
Compile time:	2018-05-16 04:38:19
MD5:	a2ac43f1303b5d26d2707d210261f391
SHA1:	ce3f01fa203ca09216a44a2e7c9326f3bf6a2d9c
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-05-16 20:45:06

URL(s) file hosting

http://www.mva.by/tags/scan%20copy84756786545.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-05-16 05:00:01	24/66	

Import library

mscoree.dll

9 Behaviors detected by system signatures

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\scan20copy84756786545.exe:Zone.Identifier

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

- Injection: scan20copy84756786545.exe(2348) -> vbc.exe(2696)

Installs itself for autorun at Windows startup

- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HkuvdD.url
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\HkuvdD.url

Checks the system manufacturer, likely for anti-virtualization

Creates a copy of itself

- copy: C:\Users\Seven01\scan20copy84756786545.exe

Creates RWX memory

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

- ioc: -7.858251E-36
- ioc: 5.483108E
- ioc: -3.06913E
- ioc: -2.639099E-33F
- ioc: 2.063778E-11F
- ioc: 4.44081E
- ioc: 1.0.0.0
- ioc: pplication.app
- ioc: asm.v2

Anomalous .NET characteristics

- anomalous_version: Assembly version is set to 0

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

- IP: 192.168.56.1:80