rrrrrr.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:	1871.50 KB (1916416 bytes)
Compile time:	2017-10-19 04:33:08
MD5:	05eee79a864f4a575bf6041bede017f7
SHA1:	5273202ab94ad184930ede395d13d6ca798fb2de
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2017-10-25 01:48:04

URL(s) file hosting

http://142.4.20.252/~kkbizint/6t/jk/rrrrrr.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2017-10-21 13:04:15	42/67	

Import library

mscoree.dll

11 Behaviors detected by system signatures

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\DwiDesk\win32.exe

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Local\Temp\.IgHiJkLiO

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\svchost
- data: C:\Users\Seven01\AppData\Local\Temp\Host.exe
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\Load
- data: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\DwiDesk\win32.lnk
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components\{6R8T0DKK-OW3T-II16-4J86-IP2QEK6ORH87}\StubPath
- data: "C:\Users\Seven01\AppData\Local\Temp\Host.exe"
- key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{6R8T0DKK-OW3T-II16-4J86-IP2QEK6ORH87}
- data: unknown

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Local\Temp\Host.exe:Zone.Identifier

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 8.00, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x001cc800, virtual_size: 0x001cc754

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\DwiDesk\win32.exe
- binary: C:\Users\Seven01\AppData\Local\Temp\Host.exe

A process created a hidden window

- Process: rrrrrr.exe -> C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\DwiDesk\win32.exe
- Process: win32.exe -> cmd

Reads data out of its own binary image

- self_read: process: rrrrrr.exe, pid: 2080, offset: 0x00000000, length: 0x001d3e00

A process attempted to delay the analysis task.

- Process: Host.exe tried to sleep 975 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

Attempts to connect to a dead IP:Port (4 unique times)

- IP: 192.168.56.1:1030
- IP: 192.168.56.1:1031
- IP: 213.183.58.34:1030 (Russian Federation)
- IP: 213.183.58.34:1031 (Russian Federation)

1 Host(s) detected

IP Address	Hostname	Reverse DNS
213.183.58.34 		

1 Countr(y|ies) detected

Hosts	Country
1	Russian Federation