out7364273.exe

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

MalFamily: Vbkryjetor **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	305.50 KB (312832 bytes)
Compile time:	2017-03-26 16:41:00
MD5:	7943cb105dd39977df534ced7c625690
SHA1:	15896fa64650cac12440f98990bd4db3a4b6ff82
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-01-29 10:31:05

URL(s) file hosting

http://mrsteamers.com/wp-content/plugins/ekro/out7364273.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-01-03 17:47:51	12/68	

Import library

mscoree.dll

28 Behaviors detected by system signatures

Collects information to fingerprint the system

Checks for the presence of known devices from debuggers and forensic tools

Detects the presence of Wine emulator via registry key

Detects Sandboxie using a known mutex

Checks the version of Bios, possibly for anti-virtualization

Detects VirtualBox using ACPI tricks

Detects VirtualBox through the presence of a device

Detects VirtualBox through the presence of a registry key

Detects VMware through the presence of a device

Detects VMware through the presence of a registry key

Detects Virtual PC using a known mutex

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\Adobe\Flash Player\AssetCache\desktop.exe

Checks for a known DeepFreeze Frozen State Mutex

Attempts to identify installed analysis tools by a known file location

- file: C:\popupkiller.exe
- file: C:\TOOLS\execute.exe

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\desktop.exe
- data: "C:\Users\Seven01\AppData\Roaming\Adobe\Flash Player\AssetCache\desktop.exe"

Attempts to repeatedly call a single API many times in order to delay analysis time

- Spam: 1ipfyoloxsookobwekoyb_output31DDCE0.exe (2472) called API GetLocalTime 34782 times
- Spam: desktop.exe (2724) called API GetLocalTime 34782 times

Tries to unhook or modify Windows functions monitored by Cuckoo

- unhook: function_name: HttpOpenRequestW, type: modification
- unhook: function_name: HttpQueryInfoA, type: modification
- unhook: function_name: HttpOpenRequestA, type: modification
- unhook: function_name: InternetConnectW, type: modification
- unhook: function_name: InternetWriteFile, type: modification
- unhook: function_name: HttpSendRequestW, type: modification
- unhook: function_name: HttpSendRequestA, type: modification
- unhook: function_name: InternetConnectA, type: modification
- unhook: function_name: InternetReadFile, type: modification
- unhook: function_name: HttpSendRequestExA, type: modification
- unhook: function_name: HttpSendRequestExW, type: modification
- unhook: function_name: InternetCloseHandle, type: modification

Deletes its original binary from disk

Detects the presence of Wine emulator via function name

Detects Sandboxie through the presence of a library

Creates RWX memory

Mimics the system's user agent string for its own requests

Repeatedly searches for a not-found process, may want to run with startbrowser=1 option

Reads data out of its own binary image

- self_read: process: 1ipfyoloxsookobwekoyb_output31DDCE0.exe, pid: 2472, offset: 0x00000000, length: 0x00059fc8

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Roaming\Adobe\Flash Player\AssetCache\desktop.exe

Performs some HTTP requests

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

Presents an Authenticode digital signature

- md5_fingerprint: a04f842754972224bd04fca25148ecb4
- sha1_fingerprint: a214f609bcf67a455e74442ab3b1d22da1354040
- cn: Repacompair Ltd
- sn: 141111799591592178956039987849183051634

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

- IP: 192.168.56.1:80

1 HTTP Request(s) detected

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

Hostname: www.download.windowsupdate.com
IP Address: 68.232.34.240
Port: 80
Count: 16