Bandios

Alföldi Mátyás

June 12, 2020

Contents

Introduction

File: Onlineinstaller.bin
VT: https://www.virustotal.com/gui/file/59c662a5207c6806046205348b22ee45da3f685fe022556716dbbd6643e61834

VT report

All the sections have an entropy of 6+, and the .rsrc section is close to 8, so there will definitely be some unpacking.
There is also a zip file, which is related to plenty of malware, but isn't detected, I would say that it is most likely password protected, like in the case of WannaCry.
It also has quite a few exports, which is rather strange for an exe.
Interesting Imports:

- GetAdaptersInfo
- Http* functions
- Internet* functions
- _TrackMouseEvent (Anti automatic sandbox analysis?)
- CreateEvent,CreateThread,CreateProcess,WaitForSingleObject combo
- Sleep (Anti vm?)
- SetUnhandledExceptionFilter+UnhandledExceptionFilter combo
- LoadLibrary* functions + GetProcAddress
- Various file operations Copy/Move/Read/Write
- Heap related functions
- Tls functions
- System information gathering
- Resource handling functions
- GetCurrentDirectory/TempPath + SetCurrentDirectory
- DuplicateHandle (possibly used as a defense mechanism)
- QueryPerformanceCounter
- IsProcessorFeaturePresent
- GetTickCount
- Service related functions
- Registry related functions
- CreateStreamOnHGlobal

- Com related functions + Variant
- File time gathering/modification

Network related:

- DNS resolution for iostream.system.band
- HTTP request to iostream.system.band/dump/io/time.php

File readings:

- Internet cache/history/cookies
- autoexec.bat
- On some systems it opens \\.\PIPE\lsarpc and \\.\PIPE\ROUTER

File modifications:

- <sys32>\spoolsr.exe
- <sys32>\MS.dat
- <sys32>\KeyHook32.dll
- <sys32>\KH.dat
- <sys32>\usp20.dll
- <sys32>\UP.dat
- <sys32>\drivers\iaStorE.sys
- <tmp>\996E.tmp

Based on the above spoolsr.exe-MS.dat KeyHook32.dll-KH.dat usp20.dll-UP.dat belong together.
The first is related to printers, and possibly data sent out for printing will be stored in MS.dat.
The second is related to keylogging.
And the driver is a defense mechanism.
Registry modifications:

- Deletes proxy related keys.
- Sets the SavedLegacySettings key

Services related:

- Creates the iaStorE service (the above mentioned driver) and also opens RASMAN

Mutexes:

- RasPbFile
- ZonesCounterMutex
- ZonesCacheCounterMutex
- ZonesLockedCacheCounterMutex

Static Analysis