Malware Analysis Report For shellcode_launcher

Binary Type

PE (Portable Executable File) (Approved)

Analyzing File

- **File Name**: shellcode_launcher
- **File Extension**: .exe
- **File Type**: EXE (Executable File).
- **MD5 Hash**: 95e15c04a8448a11490a4c02ca975acd
- **SHA256 Hash**: 5edacaca676c927246d9cf5706bb5917025ca8409c24e2af0953bbd2fcc4b8a4

File Identification

File detected as a valid Windows executable (DLL or EXE).

PE File Analysis

PE File Analysis: True

PE File Imports

- GetLastError
- LoadLibraryA
- CreateFileA
- ReadFile
- VirtualAlloc
- GetFileSize
- ExitProcess
- TerminateProcess
- GetCurrentProcess
- GetCommandLineA
- GetVersion
- WideCharToMultiByte
- MultiByteToWideChar
- LCMapStringA
- LCMapStringW
- UnhandledExceptionFilter
- GetModuleFileNameA
- FreeEnvironmentStringsA
- FreeEnvironmentStringsW
- GetEnvironmentStrings
- GetEnvironmentStringsW
- SetHandleCount
- GetStdHandle
- GetFileType

- GetStartupInfoA
- GetModuleHandleA
- GetEnvironmentVariableA
- GetVersionExA
- HeapDestroy
- HeapCreate
- VirtualFree
- HeapFree
- RtlUnwind
- WriteFile
- HeapAlloc
- GetStringTypeA
- GetStringTypeW
- GetCPInfo
- GetACP
- GetOEMCP
- HeapReAlloc
- GetProcAddress
- FlushFileBuffers
- SetFilePointer
- SetStdHandle
- CloseHandle

PE File Exports

No Exported functions were found.

String Analysis

ASCII Strings

- !This program cannot be run in DOS mode.
- `.rdata
- @.data
- ^}%95,
- HHtpHHtl
- [ShDq@
- "WWSh@q@
- SS@SSPVSS
- t#SSUP
- t$$VSS
- _^][YY
- DSUVWh
- t.;t$$t(
- VC20XC00U
- ^VhDq@
- PVh@q@
- `h````
- ppxxxx
- (null)
- _*GLOBAL*HEAP_SELECTED
- _*MSVCRT*HEAP_SELECT

- runtime error
- TLOSS error
- SING error
- DOMAIN error
-
    - unable to initialize heap
-
    - not enough space for lowio initialization
-
    - not enough space for stdio initialization
-
    - pure virtual function call
-
    - not enough space for *onexit/atexit table*
-
    - *unable to open console device*
-
    - *unexpected heap error*
-
    - *unexpected multithread lock error*
-
    - *not enough space for thread data*
- *abnormal program termination*
-
    - *not enough space for environment*
-
    - *not enough space for arguments*
-
    - *floating point not loaded*
- *Microsoft Visual C++ Runtime Library*
- *Runtime Error!*
- *Program:*
-
- *GetLastActivePopup*
- *GetActiveWindow*
- *MessageBoxA*
- *user32.dll*
- *GetLastError*
- *LoadLibraryA*
- *CreateFileA*
- *ReadFile*
- *VirtualAlloc*
- *GetFileSize*
- *KERNEL32.dll*
- *ExitProcess*
- *TerminateProcess*
- *GetCurrentProcess*
- *GetCommandLineA*
- *GetVersion*
- *WideCharToMultiByte*
- *MultiByteToWideChar*

- *LCMapStringA*
- *LCMapStringW*
- *UnhandledExceptionFilter*
- *GetModuleFileNameA*
- *FreeEnvironmentStringsA*
- *FreeEnvironmentStringsW*
- *GetEnvironmentStrings*
- *GetEnvironmentStringsW*
- *SetHandleCount*
- *GetStdHandle*
- *GetFileType*
- *GetStartupInfoA*
- *GetModuleHandleA*
- *GetEnvironmentVariableA*
- *GetVersionExA*
- *HeapDestroy*
- *HeapCreate*
- *VirtualFree*
- *HeapFree*
- *RtlUnwind*
- *WriteFile*
- *HeapAlloc*
- *GetStringTypeA*
- *GetStringTypeW*
- *GetCPInfo*
- *GetACP*
- *GetOEMCP*
- *HeapReAlloc*
- *GetProcAddress*
- *FlushFileBuffers*
- *SetFilePointer*
- *SetStdHandle*
- *CloseHandle*
- *X[YZ^*
- -L : Load library during initialization
- -bp: add a breakpoint prior to jumping into the shellcode
- +: load register with a pointer to the end of the shellcode
- -: load register with a pointer to the start of the shellcode
- requires an open handle for
- or writeable (-w), such as for a malicious PDF the shellcode
- is an additional file to open, either readonly (-r)
- is the (decimal) offset into the shellcode to start executing
- is the binary containing the shellcode to execute
- shellcode*launcher.exe -i -o [-bp] [-r]*
- *[-w] [-L name] [-][+]*
- *Usage: shellcode_launcher.exe*
- *Missing argument to %s*
- *Error loading library %s: 0x%08*
- *Trying to LoadLibrary: %s*
- *Opening read-writeable file: %s*
- *Opening writeable file: %s*
- *Couldn't open file %s: %08x*

- *Opening readable file: %s*
- *Only read %d of %d bytes!*
- *Couldn't read file bytes*
- *Couldn't allocate %d bytes*
- *Execution offset larger than file size!*
- *Couldn't get file size*
- *Couldn't open shellcode-containing file %s: %08x*
- *ERROR: no output buffer specified*
- *Setting pop %d at 0x%08x*
- *Setting reg start: %08x %08x %d*
- *Setting reg end: %08x %08x %d*
- *Creating breakpoint at: 0x%08x*
- *Error during doSetBp*
- *Error during doSetRegEnd*
- *Error during doSetRegStart*
- *ERROR: bad args to fillPreambleBuffer*
- *WARNING: unknown flag: %s. Skipping*
- *Setting %d +%s*
- *Setting %d -%s*
- *ERROR: conflicting +/- requests for register %s*
- *ERROR: Too many -rwfiles specified. Limit is %d*
- *ERROR: Too many -wfiles specified. Limit is %d*
- *ERROR: Too many -r files specified. Limit is %d*
- *Using starting offset: 0x%08x (%d)*
- *Calling file now. Loaded binary at: 0x%08x*
- *Filling preamble buffer failed. Exiting*
- *Creating shellcode buffer failed. Exiting*
- *Creat auxiliary files failed. Exiting*
- *Load Libraries failed. Exiting*
- *Starting up*

UTF-8 Strings

No detected.

UTF-16LE Strings

- *(null)*
- *(((((H*

Extracted URLs

No detected.

Base64 Strings

No valid Base64-encoded strings found.

File Entropy Analysis

- ***Entropy**: `4.52`*
- ***Status**: This file likely contains Standard Text or human-readable text.*

VirusTotal Analysis

***Scan Date**: 2024-10-02 21:47:35*

Scan Results

- *Malicious: 37*
- *Suspicious: 0*
- *Undetected: 35*
- *Harmless: 0*
- *Timeout: 0*
- *Confirmed-timeout: 0*
- *Failure: 0*
- *Type-unsupported: 4*

Community Votes

- *Harmless: 0*
- *Malicious: 0*

Detailed Engine Results

Engine Name	Detection Category	Detection
Bkav	malicious	W32.Common.1581A828
Lionic	malicious	Trojan.Win32.ShellExec.4!c
MicroWorld-eScan	malicious	Gen:Variant.Fragtor.371462
FireEye	malicious	Gen:Variant.Fragtor.371462
CAT-QuickHeal	malicious	PUA.ShellexecRl.S18206443
VIPRE	malicious	Gen:Variant.Fragtor.371462
BitDefender	malicious	Gen:Variant.Fragtor.371462
CrowdStrike	malicious	win/grayware*confidence*60% (D)
huorong	malicious	VirTool/Meterpreter.c
Symantec	malicious	Trojan.Gen.2
ESET-NOD32	malicious	a variant of Win32/RiskWare.ShellExec.D
Paloalto	malicious	generic.ml
Alibaba	malicious	RiskWare:Win32/ShellExec.352312f9
Rising	malicious	Trojan.Win32.Generic.18145192 (C64:YzY0Ogst9Xmsyjlc)
Emsisoft	malicious	Gen:Variant.Fragtor.371462 (B)
Zillya	malicious	Tool.ShellExec.Win32.134
Sophos	malicious	ATK/ShellLnch-A
Ikarus	malicious	Trojan.SuspectCRC
Varist	malicious	W32/ABRisk.ZAOA-1664
Antiy-AVL	malicious	RiskWare/Win32.ShellExec

Engine Name	Detection Category	Detection
Kingsoft	malicious	Win32.Troj.Unknown.a
Xcitium	malicious	Malware@#1ql4jgzkmfeg9
Arcabit	malicious	Trojan.Fragtor.D5AB06
GData	malicious	Gen:Variant.Fragtor.371462
ALYac	malicious	Gen:Variant.Fragtor.371462
Malwarebytes	malicious	Malware.AI.3401867953
TrendMicro-HouseCall	malicious	TROJ_GEN.R014H0CGB23
Yandex	malicious	RiskWare.ShellExec!GUZd1iEm1Hw
CTX	malicious	exe.unknown.fragtor
MaxSecure	malicious	Trojan.Malware.226584847.susgen
Fortinet	malicious	Generik.EPACZOK!tr
AVG	malicious	Win32:Malware-gen
Avast	malicious	Win32:Malware-gen
alibabacloud	malicious	RiskWare:Win/ShellExec.D