Malware Analysis Report For Lab10-03

Binary Type

PE (Portable Executable File) (Approved)

Analyzing File

- **File Name**: Lab10-03
- **File Extension**: .exe
- **File Type**: EXE (Executable File).
- **MD5 Hash**: f72d773f13ceb6b842a9d29c56f8880f
- **SHA256 Hash**: d66e15eea51ebd4bfd13f8c97646253740b1e6a99328d22232fd01ae13ef5d05

File Identification

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

PE File Analysis

PE File Analysis: True

PE File Imports

- CreateFileA
- DeviceIoControl
- Sleep
- GetStringTypeA
- LCMapStringW
- LCMapStringA
- MultiByteToWideChar
- LoadLibraryA
- GetProcAddress
- GetModuleHandleA
- GetStartupInfoA
- GetCommandLineA
- GetVersion
- ExitProcess
- TerminateProcess
- GetCurrentProcess
- UnhandledExceptionFilter
- GetModuleFileNameA
- FreeEnvironmentStringsA
- FreeEnvironmentStringsW
- WideCharToMultiByte
- GetEnvironmentStrings
- GetEnvironmentStringsW
- SetHandleCount

- GetStdHandle
- GetFileType
- HeapDestroy
- HeapCreate
- VirtualFree
- HeapFree
- RtlUnwind
- WriteFile
- GetCPInfo
- GetACP
- GetOEMCP
- HeapAlloc
- VirtualAlloc
- HeapReAlloc
- GetStringTypeW
- CloseServiceHandle
- OpenSCManagerA
- CreateServiceA
- StartServiceA
- CoCreateInstance
- OleUninitialize
- OleInitialize
- SysAllocString
- VariantInit

PE File Exports

No Exported functions were found.

String Analysis

ASCII Strings

- !This program cannot be run in DOS mode.
-)RichH
- `.rdata
- @.data
- T$,RVP
- YYh P@
- SS@SSPVSS
- t#SSUP
- t$$VSS
- _^][YY
- DSUVWh
- t.;t$$t(
- VC20XC00U
- [Sh,D@
- "WWSh(D@
- ^Vh,D@
- PVh(D@
- 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
- DeviceIoControl
- CreateFileA
- KERNEL32.dll
- CloseServiceHandle
- StartServiceA
- CreateServiceA
- OpenSCManagerA
- ADVAPI32.dll
- OleUninitialize
- CoCreateInstance
- OleInitialize
- ole32.dll
- OLEAUT32.dll
- GetModuleHandleA
- GetStartupInfoA
- GetCommandLineA

- GetVersion
- ExitProcess
- TerminateProcess
- GetCurrentProcess
- UnhandledExceptionFilter
- GetModuleFileNameA
- FreeEnvironmentStringsA
- FreeEnvironmentStringsW
- WideCharToMultiByte
- GetEnvironmentStrings
- GetEnvironmentStringsW
- SetHandleCount
- GetStdHandle
- GetFileType
- HeapDestroy
- HeapCreate
- VirtualFree
- HeapFree
- RtlUnwind
- WriteFile
- GetCPInfo
- GetACP
- GetOEMCP
- HeapAlloc
- VirtualAlloc
- HeapReAlloc
- GetProcAddress
- LoadLibraryA
- MultiByteToWideChar
- LCMapStringA
- LCMapStringW
- GetStringTypeA
- GetStringTypeW
- \.\ProcHelper
- Process Helper
- C:\Windows\System32\Lab10-03.sys

UTF-8 Strings

No detected.

UTF-16LE Strings

- http://www.malwareanalysisbook.com/ad.html
- (((((H

Extracted URLs

- http://www.malwareanalysisbook.com/ad.html

Base64 Strings

No valid Base64-encoded strings found.

File Entropy Analysis

- **Entropy**: `4.38`
- **Status**: This file likely contains Standard Text or human-readable text.

VirusTotal Analysis

Scan Date: 2024-10-01 17:07:04

Scan Results

- Malicious: 31
- Suspicious: 0
- Undetected: 41
- Harmless: 0
- Timeout: 0
- Confirmed-timeout: 0
- Failure: 0
- Type-unsupported: 4

Community Votes

- Harmless: 0
- Malicious: 1

Detailed Engine Results

Engine Name	Detection Category	Detection
Bkav	malicious	W32.AIDetectMalware
Lionic	malicious	Trojan.Win32.Generik.4!c
Skyhigh	malicious	RDN/Generic.dx
McAfee	malicious	RDN/Generic.dx
Malwarebytes	malicious	Generic.Malware/Suspicious
Alibaba	malicious	Trojan:Win32/Generic.13737390
huorong	malicious	Trojan/ServStart.x
Paloalto	malicious	generic.ml
Symantec	malicious	Trojan.Gen.MBT
ESET-NOD32	malicious	a variant of Generik.HJSNDKX
Avast	malicious	Win32:Trojan-gen
NANO-Antivirus	malicious	Trojan.Win32.Generik.dxhdek
Sophos	malicious	Mal/Generic-S
DrWeb	malicious	Trojan.Siggen8.36843
McAfeeD	malicious	ti!D66E15EEA51E
Trapmine	malicious	suspicious.low.ml.score

Engine Name	Detection Category	Detection
Ikarus	malicious	Trojan.SuspectCRC
Varist	malicious	W32/ABRisk.QPIF-5888
Antiy-AVL	malicious	Trojan/Win32.SGeneric
Kingsoft	malicious	Win32.Troj.Unknown.a
Gridinsoft	malicious	Trojan.Win32.Agent.oa!s1
Xcitium	malicious	Malware@#nd1154j1nxrp
VBA32	malicious	Adware.Presenoker
TrendMicro-HouseCall	malicious	TROJ_GEN.R002H06FT23
Rising	malicious	Malware.Undefined!8.C (TFE:5:AvtTWPMGk6L)
AVG	malicious	Win32:Trojan-gen
alibabacloud	malicious	Trojan:Win/ServStart.XZ