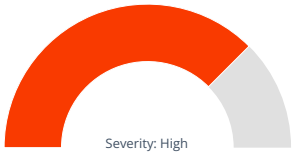
VALKYRIE COMODO

Summary

File Name: LixoDestructive.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 2add11e25d07dc9e154ae1be916c869804047146
MD5: 7d538a430eb4e0bfd7671b921a8b76a1

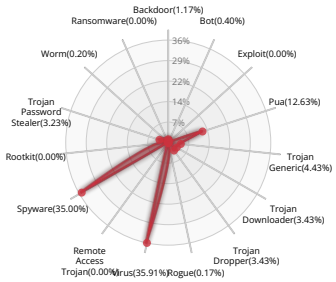
MALWARE
Valkyrie Final Verdict

DETECTION SECTION

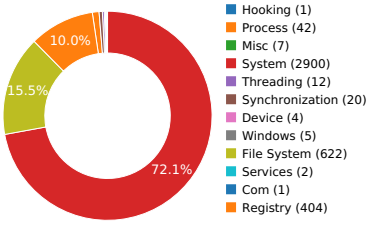


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

STEALING OF SENSITIVE INFORMATION

Attempts to modify Internet Explorer's start page — Show sources

MALWARE ANALYSIS SYSTEM EVASION

Network activity detected but not expressed in API logs

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

Likely virus infection of existing system binary — Show sources

VALKYRIE COMODO

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES
C:\Users\user\AppData\Local\Temp\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\System32\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\system\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\api-ms-win-core-fibers-l1-1-1.DLL
C:\ProgramData\Oracle\Java\javapath\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\System32\wbem\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Universal Extractor\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-core-fibers-l1-1-1.DLL
C:\Python27\api-ms-win-core-fibers-l1-1-1.DLL
C:\Python27\Scripts\api-ms-win-core-fibers-l1-1-1.DLL
C:\tools\sysinternals\api-ms-win-core-fibers-l1-1-1.DLL
C:\tools\api-ms-win-core-fibers-l1-1-1.DLL
C:\tools\IDA_Pro_v6\python\api-ms-win-core-fibers-l1-1-1.DLL
C:\Users\user\AppData\Local\Temp\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\System32\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\system\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\api-ms-win-core-localization-l1-2-1.DLL
C:\ProgramData\Oracle\Java\javapath\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\System32\wbem\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-core-localization-l1-2-1.DLL
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-core-localization-l1-2-1.DLL
C:\Program Files (x86)\Universal Extractor\api-ms-win-core-localization-l1-2-1.DLL
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-core-localization-l1-2-1.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-core-localization-l1-2-1.DLL
C:\Python27\api-ms-win-core-localization-l1-2-1.DLL
C:\Python27\Scripts\api-ms-win-core-localization-l1-2-1.DLL
C:\tools\sysinternals\api-ms-win-core-localization-l1-2-1.DLL
C:\tools\api-ms-win-core-localization-l1-2-1.DLL
C:\tools\IDA_Pro_v6\python\api-ms-win-core-localization-l1-2-1.DLL
C:\Windows\WinNet.exe
C:\Windows\Fonts\staticcache.dat
\Device\KsecDD
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\System32\Scanner.exe
C:\Windows\calc.exe
C:\Users\user\AppData\Local\Temp\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Windows\System32\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Windows\system\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Windows\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\ProgramData\Oracle\Java\javapath\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Windows\System32\wbem\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Program Files (x86)\Universal Extractor\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-core-sysinfo-l1-2-1.DLL
C:\Python27\api-ms-win-core-sysinfo-l1-2-1.DLL

C:\Python27\Scripts\api-ms-win-core-sysinfo-l1-2-1.DLL

C:\tools\sysinternals\api-ms-win-core-sysinfo-l1-2-1.DLL

C:\tools\api-ms-win-core-sysinfo-l1-2-1.DLL

C:\tools\IDA_Pro_v6\python\api-ms-win-core-sysinfo-l1-2-1.DLL

C:\Windows\System32\tzres.dll

\??\PhysicalDrive0

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c

C:\Users\user\AppData\Local\Temp\This is just the beginning my friend!

C:\Users\user\AppData\Local\Temp\his is just the beginning my friend!

C:\Users\user\AppData\Local\Temp\is is just the beginning my friend!

C:\Users\user\AppData\Local\Temp\s is just the beginning my friend!

C:\Users\user\AppData\Local\Temp\ is just the beginning my friend!

C:\Users\user\AppData\Local\Temp\is just the beginning my friend!

C:\Users\user\AppData\Local\Temp\s just the beginning my friend!

C:\Users\user\AppData\Local\Temp\ just the beginning my friend!

C:\Users\user\AppData\Local\Temp\just the beginning my friend!

C:\Users\user\AppData\Local\Temp\ust the beginning my friend!

C:\Users\user\AppData\Local\Temp\st the beginning my friend!

C:\Users\user\AppData\Local\Temp\t the beginning my friend!

C:\Users\user\AppData\Local\Temp\ the beginning my friend!

C:\Users\user\AppData\Local\Temp\the beginning my friend!

C:\Users\user\AppData\Local\Temp\he beginning my friend!

C:\Users\user\AppData\Local\Temp\e beginning my friend!

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave2
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave3
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave4
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave5
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave6
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave7
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave8
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave9
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi2
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi3
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi4
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi5
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi6
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi7
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi8
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi9
HKEY_CURRENT_USER\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm\wheel
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wdmaud.drv
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\SYSTEM\Setup\SystemSetupInProgress
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{a45c254e-df1c-4efd-8020-67d146a850e0},2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{026e516e-b814-414b-83cd-856d6fef4822},2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{1da5d803-d492-4edd-8c23-e0c0ffee7f0e},0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\NdrOleExtDLL
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{d39cf7fb-6b16-44c3-a019-e218374ed1f1}\Properties\{a45c254e-df1c-4efd-8020-67d146a850e0},2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{d39cf7fb-6b16-44c3-a019-e218374ed1f1}\Properties\{026e516e-b814-414b-83cd-856d6fef4822},2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{d39cf7fb-6b16-44c3-a019-e218374ed1f1}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{d39cf7fb-6b16-44c3-a019-e218374ed1f1}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{d39cf7fb-6b16-44c3-a019-e218374ed1f1}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{d39cf7fb-6b16-44c3-a019-e218374ed1f1}\Properties\{1da5d803-d492-4edd-8c23-e0c0ffee7f0e},0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Capture\{8afafb6a-f1b0-4935-be8a-5894d19191bd}\Properties\{a45c254e-df1c-4efd-8020-67d146a850e0},2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Capture\{8afafb6a-f1b0-4935-be8a-5894d19191bd}\Properties\{026e516e-b814-414b-83cd-856d6fef4822},2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Capture\{8afafb6a-f1b0-4935-be8a-5894d19191bd}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Capture\{8afafb6a-f1b0-4935-be8a-5894d19191bd}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Capture\{8afafb6a-f1b0-4935-be8a-5894d19191bd}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Capture\{8afafb6a-f1b0-4935-be8a-5894d19191bd}\Properties\{1da5d803-d492-4edd-8c23-e0c0ffee7f0e},0
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wavemapper
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midimapper
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\DeviceState
HKEY_CURRENT_USER\Software\Microsoft\Multimedia\Audio\UserDuckingPreference

MODIFIED FILES

C:\Windows\System32\Scanner.exe
C:\Windows\calc.exe
\??\PhysicalDrive0
C:\Users\user\AppData\Local\Temp\This is just the beginning my friend!

C:\Users\user\AppData\Local\Temp\his is just the beginning my friend!
C:\Users\user\AppData\Local\Temp\is is just the beginning my friend!
C:\Users\user\AppData\Local\Temp\s is just the beginning my friend!
C:\Users\user\AppData\Local\Temp\ is just the beginning my friend!
C:\Users\user\AppData\Local\Temp\is just the beginning my friend!
C:\Users\user\AppData\Local\Temp\s just the beginning my friend!
C:\Users\user\AppData\Local\Temp\ just the beginning my friend!
C:\Users\user\AppData\Local\Temp\just the beginning my friend!
C:\Users\user\AppData\Local\Temp\ust the beginning my friend!
C:\Users\user\AppData\Local\Temp\st the beginning my friend!
C:\Users\user\AppData\Local\Temp\t the beginning my friend!
C:\Users\user\AppData\Local\Temp\ the beginning my friend!
C:\Users\user\AppData\Local\Temp\the beginning my friend!
C:\Users\user\AppData\Local\Temp\he beginning my friend!
C:\Users\user\AppData\Local\Temp\e beginning my friend!
C:\Users\user\AppData\Local\Temp\ beginning my friend!
C:\Users\user\AppData\Local\Temp\beginning my friend!
C:\Users\user\AppData\Local\Temp\eginning my friend!
C:\Users\user\AppData\Local\Temp\ginning my friend!
C:\Users\user\AppData\Local\Temp\inning my friend!
C:\Users\user\AppData\Local\Temp\nning my friend!
C:\Users\user\AppData\Local\Temp\ning my friend!
C:\Users\user\AppData\Local\Temp\ing my friend!
C:\Users\user\AppData\Local\Temp\ng my friend!
C:\Users\user\AppData\Local\Temp\g my friend!
C:\Users\user\AppData\Local\Temp\ my friend!
C:\Users\user\AppData\Local\Temp\my friend!
C:\Users\user\AppData\Local\Temp\y friend!
C:\Users\user\AppData\Local\Temp\ friend!
C:\Users\user\AppData\Local\Temp\friend!
C:\Users\user\AppData\Local\Temp\riend!
C:\Users\user\AppData\Local\Temp\iend!
C:\Users\user\AppData\Local\Temp\end!
C:\Users\user\AppData\Local\Temp\nd!
C:\Users\user\AppData\Local\Temp\d!
C:\Users\user\AppData\Local\Temp\!
C:\Users\user\AppData\Local\Temp\Lixo.exe - ur fucked up
C:\Users\user\AppData\Local\Temp\ixo.exe - ur fucked up
C:\Users\user\AppData\Local\Temp\xo.exe - ur fucked up
C:\Users\user\AppData\Local\Temp\o.exe - ur fucked up
C:\Users\user\AppData\Local\Temp\.exe - ur fucked up
C:\Users\user\AppData\Local\Temp\exe - ur fucked up
C:\Users\user\AppData\Local\Temp\xe - ur fucked up
C:\Users\user\AppData\Local\Temp\e - ur fucked up
C:\Users\user\AppData\Local\Temp\ - ur fucked up
C:\Users\user\AppData\Local\Temp\- ur fucked up
C:\Users\user\AppData\Local\Temp\ ur fucked up
C:\Users\user\AppData\Local\Temp\ur fucked up
C:\Users\user\AppData\Local\Temp\r fucked up
C:\Users\user\AppData\Local\Temp\ fucked up
C:\Users\user\AppData\Local\Temp\fucked up
C:\Users\user\AppData\Local\Temp\ucked up

C:\Users\user\AppData\Local\Temp\cked up
C:\Users\user\AppData\Local\Temp\ked up
C:\Users\user\AppData\Local\Temp\ed up
C:\Users\user\AppData\Local\Temp\d up
C:\Users\user\AppData\Local\Temp\ up
C:\Users\user\AppData\Local\Temp\up
C:\Users\user\AppData\Local\Temp\p
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\Pneumonoultramicroscopicosilicovolcanoconiosis
C:\Users\user\AppData\Local\Temp\neumonoultramicroscopicosilicovolcanoconiosis
C:\Users\user\AppData\Local\Temp\eumonoultramicroscopicosilicovolcanoconiosis
C:\Users\user\AppData\Local\Temp\umonoultramicroscopicosilicovolcanoconiosis
C:\Users\user\AppData\Local\Temp\monoultramicroscopicosilicovolcanoconiosis
C:\Users\user\AppData\Local\Temp\onoultramicroscopicosilicovolcanoconiosis
C:\Users\user\AppData\Local\Temp\noultramicroscopicosilicovolcanoconiosis
C:\Users\user\AppData\Local\Temp\oultramicroscopicosilicovolcanoconiosis
C:\Users\user\AppData\Local\Temp\ultramicroscopicosilicovolcanoconiosis
C:\Users\user\AppData\Local\Temp\ltramicroscopicosilicovolcanoconiosis
C:\Users\user\AppData\Local\Temp\tramicroscopicosilicovolcanoconiosis
C:\Users\user\AppData\Local\Temp\ramicroscopicosilicovolcanoconiosis

RESOLVED APIS

kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.FlsAlloc
kernel32.dll.FlsSetValue
kernel32.dll.FlsGetValue
kernel32.dll.LCMapStringEx
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
gdi32.dll.GetTextFaceAliasW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
gdi32.dll.GetFontAssocStatus
advapi32.dll.RegQueryValueExA
advapi32.dll.RegEnumKeyExW
dwmapi.dll.DwmIsCompositionEnabled
gdi32.dll.GdiIsMetaPrintDC
ole32.dll.CoInitializeEx
ole32.dll.CoUninitialize
cryptbase.dll.SystemFunction036
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoRevokeInitializeSpy
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
sechost.dll.OpenSCManagerW
sechost.dll.OpenServiceW
sechost.dll.QueryServiceStatus
sechost.dll.CloseServiceHandle
rpcrt4.dll.RpcStringBindingComposeW

rpcrt4.dll.RpcBindingFromStringBindingW
rpcrt4.dll.RpcStringFreeW
mmdevapi.dll.#3
wdmaud.drv.DriverProc
wdmaud.drv.modMessage
wdmaud.drv.midMessage
rpcrt4.dll.NdrClientCall2
wdmaud.drv.wodMessage
mmdevapi.dll.DllGetClassObject
ole32.dll.CoCreateFreeThreadedMarshaler
setupapi.dll.SetupDiCreateDeviceInfoList
kernel32.dll.RegOpenKeyExW
kernel32.dll.RegCloseKey
wdmaud.drv.mxdMessage
ole32.dll.CoTaskMemAlloc
shlwapi.dll.#487
ole32.dll.CoTaskMemFree
ole32.dll.PropVariantClear
setupapi.dll.SetupDiOpenDeviceInfoW
setupapi.dll.SetupDiGetDeviceInstanceIdW
setupapi.dll.SetupDiGetDevicePropertyW
shlwapi.dll.SHStrDupW
audioses.dll.DllGetClassObject
ole32.dll.NdrOleInitializeExtension
ole32.dll.CoGetClassObject
ole32.dll.CoGetMarshalSizeMax
ole32.dll.CoMarshalInterface
ole32.dll.CoUnmarshalInterface
ole32.dll.StringFromIID
ole32.dll.CoGetPSClsid
ole32.dll.CoCreateInstance
ole32.dll.CoReleaseMarshalData
ole32.dll.DcomChannelSetHResult
wdmaud.drv.widMessage
msacm32.drv.DriverProc
msacm32.drv.wodMessage
msacm32.drv.widMessage
midimap.dll.DriverProc
midimap.dll.modMessage

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\2add11e25d07dc9e154ae1be916c869804047146.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\DRIVERS32
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave2
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave3
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave4
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave5
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave6
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave7
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave8
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave9
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi2
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi3
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi4
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi5
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi6
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi7
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi8
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi9
HKEY_CURRENT_USER\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm
HKEY_CURRENT_USER\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm\wheel

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wdmaud.drv

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode

HKEY_LOCAL_MACHINE\System\Setup

HKEY_LOCAL_MACHINE\SYSTEM\Setup\SystemSetupInProgress

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{a45c254e-df1c-4efd-8020-67d146a850e0},2

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{026e516e-b814-414b-83cd-856d6fef4822},2

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},2

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},6

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},1

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{1da5d803-d492-4edd-8c23-e0c0ffee7f0e},0

READ FILES

C:\Windows\Fonts\staticcache.dat

\Device\KsecDD

C:\Windows\Globalization\Sorting\sortdefault.nls

C:\Windows\System32\tzres.dll

\??\PhysicalDrive0

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\

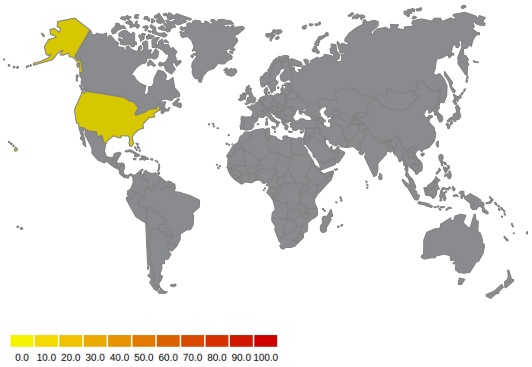
C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\
C:\Users\user\AppData\Local\Temp\2add11e25d07dc9e1\xee\xb0\x8c\xea\xb7\x8f\xef\x8f\xa0=\xea\xa3\xb3\xe7\x9e\x88\xef\x9f\xb4=\xe4\x84\x8e\xe7\x9a\x8f\xe5\xaa\x90\xed\xad\xb5\xef\xbf\xbe\xef\xbf\xbf\xe4\x83\xba\xe7\x9a\x87\xe3\xaf\x9c\
C:\Windows\System32\en-US\wdmaud.drv.mui
C:\Windows\System32\en-US\MMDevAPI.DLL.mui

MUTEXES

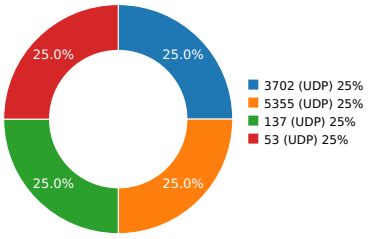
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	142.251.41.14	United States	15169	Google LLC	Malware Process
	142.251.40.174	United States	15169	Google LLC	Malware Process
	142.251.40.142	United States	15169	Google LLC	Malware Process
	142.251.40.110	United States	15169	Google LLC	Malware Process
	142.251.35.174	United States	15169	Google LLC	Malware Process
	142.251.32.110	United States	15169	Google LLC	Malware Process
	142.250.81.238	United States	15169	Google LLC	Malware Process
	142.250.80.78	United States	15169	Google LLC	Malware Process
	142.250.80.46	United States	15169	Google LLC	Malware Process
	142.250.80.14	United States	15169	Google LLC	Malware Process
	142.250.80.110	United States	15169	Google LLC	Malware Process
	142.250.65.238	United States	15169	Google LLC	Malware Process
	142.250.65.206	United States	15169	Google LLC	Malware Process
	142.250.65.174	United States	15169	Google LLC	Malware Process
	142.250.64.78	United States	15169	Google LLC	Malware Process
www.youtube.com	142.250.72.110	United States	15169	Google LLC	Malware Process

DNS QUERIES

Request	Type
www.youtube.com	A

Answers
- 142.250.65.238 (A)
- 142.251.40.110 (A)
- 142.251.32.110 (A)
- 142.250.80.14 (A)
- 142.251.35.174 (A)
- 142.250.65.174 (A)
- youtube-ui.l.google.com (CNAME)
- 142.250.72.110 (A)
- 142.251.41.14 (A)
- 142.250.65.206 (A)
- 142.250.64.78 (A)
- 142.250.80.78 (A)
- 142.251.40.142 (A)
- 142.251.40.174 (A)
- 142.250.80.110 (A)
- 142.250.80.46 (A)
- 142.250.81.238 (A)

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
-1.74859285355	Sandbox	192.168.56.255	137
-0.490409851074	Sandbox	224.0.0.252	5355
3.53992319107	Sandbox	239.255.255.250	3702
42.7684600353	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	LixoDestructive.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	2add11e25d07dc9e154ae1be916c869804047146
MD5:	7d538a430eb4e0bfd7671b921a8b76a1
First Seen Date:	2023-05-02 13:15:25.025559 (2 days ago)
Number Of Clients Seen:	4
Last Analysis Date:	2023-05-03 18:55:31.338920 (about 22 hours ago)
Human Expert Analysis Date:	2023-05-02 21:21:43.172170 (2 days ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	6
Trid	[]
Compilation Time Stamp	0x64223EF1 [Tue Mar 28 01:12:17 2023 UTC]
Entry Point	0x407f6d (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	484352
Ssdeep	
Sha256	3a4ea5e72e50bcba550efa034818f35785076adb37af4c1cee9374fe9e013ec1
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x489d0	0x48a00	6.63352370442	dd7150650ce709ab2dc703342af33dc7
.rdata	0x4a000	0xf69c	0xf800	5.75183497883	7c186d4c6b5714ed3bf4f4f081dd4755
.data	0x5a000	0x1cf0	0xa00	2.46526476329	0fe90a099face26e50573e8f8f491640
.msvcjmc	0x5c000	0x16	0x200	0.255742020076	85bb7567c9540c02a36ab2534359c3af
.rsrc	0x5d000	0x1a4b8	0x1a600	5.95991151638	a4944c494e0465bf8a3bac0c21fd686c
.reloc	0x78000	0x2b60	0x2c00	6.69701565351	e0240d393546e7014d03aa140aacd7ef

PE Resources

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 381408, u'sha256': u'df895c32df681f3c40a0fbf75b1a40c39aac578d5f2480be5e9c8982890d3609', u'type': u'dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0', u'size': 67624}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 449032, u'sha256': u'7e5f3613909ed5ea12f5df405a9c06e86ee54c58a5d4efe7e2d91bf26279e15a', u'type': u'data', u'size': 21640}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 470672, u'sha256': u'ea46ba71e5d30cbf907e14a83f1468d27ce32a9416d9e7809deb68b3a91d6cc9', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 480312, u'sha256': u'8b80a88109482ae2999aa3c262e714f82af67df486c1448b2290a11b66a559c1', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 484576, u'sha256': u'1e83fd803d10345f0e8c059f73b3fc58d4ef719ed3fc227b15b4e2713296070b', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 487016, u'sha256': u'59fb53a712b6feee73b4105635de9cb554ac11e10ec6b58c6f6d61c8fd45f15e', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

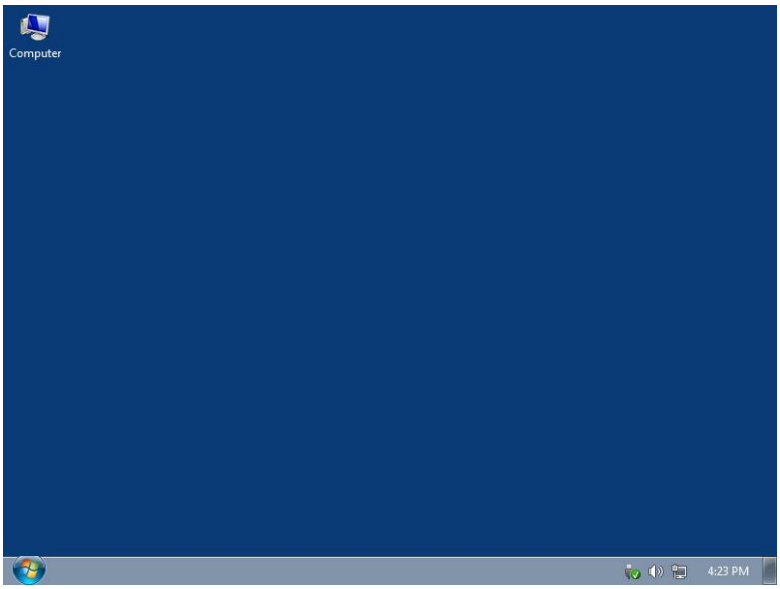
{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_GROUP_ICON', u'offset': 488144, u'sha256': u'66b4d37d44fbf4d63b7a9a748f7ee25168874e222c889ace2eacbff42c028374', u'type': u'MS Windows icon resource - 6 icons, 128x128', u'size': 90}

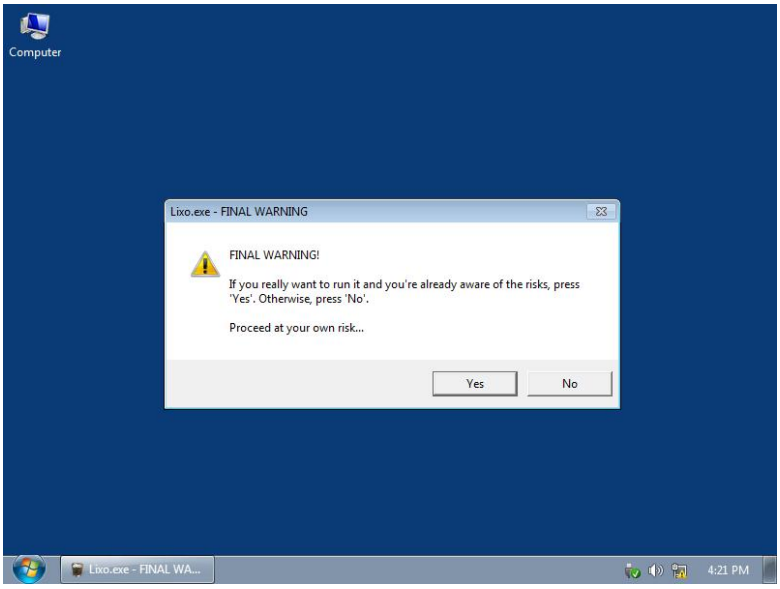
{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 488240, u'sha256': u'165c5c883fd4fd36758bcba6baf2faffb77d2f4872ffd5ee918a16f91de5a8a8', u'type': u'XML 1.0 document text', u'size': 392}

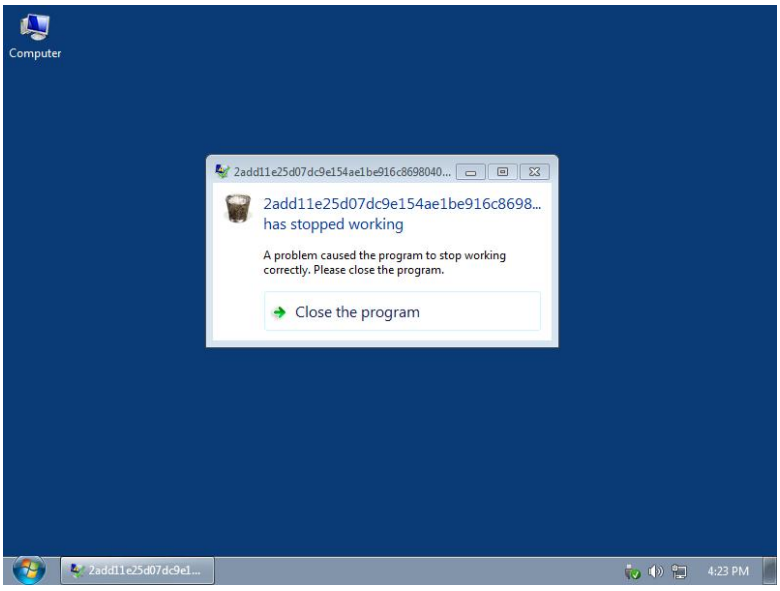
CERTIFICATE VALIDATION

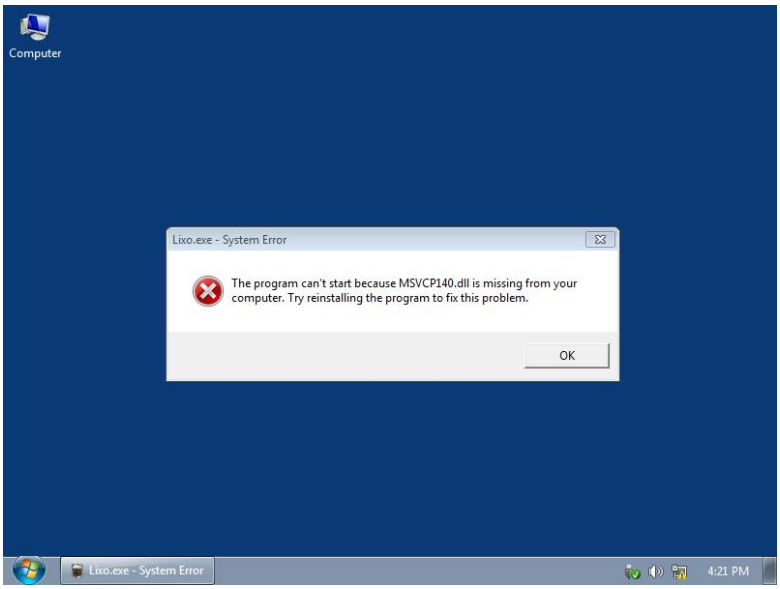
- Certificate Validation is not Applicable ?

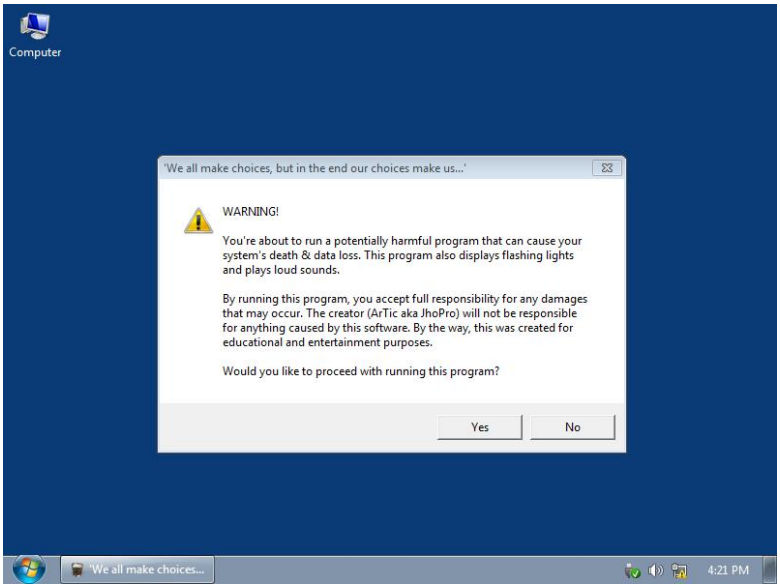
SCREENSHOTS


Computer
4:23 PM


Computer
Lixo.exe - FINAL WARNING
FINAL WARNING!
If you really want to run it and you're already aware of the risks, press 'Yes'. Otherwise, press 'No'.
Proceed at your own risk...
Yes
No
Lixo.exe - FINAL WA...
4:21 PM


Computer
2add11e25d07dc9e154ae1be916c8698040...
2add11e25d07dc9e154ae1be916c8698...
has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
2add11e25d07dc9e1...
4:23 PM


Computer
Lixo.exe - System Error
The program can't start because MSVCP140.dll is missing from your computer. Try reinstalling the program to fix this problem.
OK
Lixo.exe - System Error
4:21 PM


Computer
'We all make choices, but in the end our choices make us...'
WARNING!
You're about to run a potentially harmful program that can cause your system's death & data loss. This program also displays flashing lights and plays loud sounds.
By running this program, you accept full responsibility for any damages that may occur. The creator (ArTic aka JhoPro) will not be responsible for anything caused by this software. By the way, this was created for educational and entertainment purposes.
Would you like to proceed with running this program?
Yes
No
'We all make choices...
4:21 PM


Computer
4:21 PM


Computer
4:21 PM


Computer
4:21 PM