Summary

File Name: fe3658635c66bb8b0981fe3f73cebf1b229ed661

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

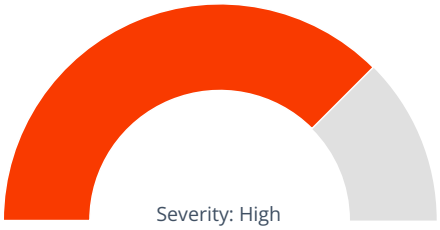
SHA1: fe3658635c66bb8b0981fe3f73cebf1b229ed661

MD5: a48de889c19197426214da54922eb7ad

MALWARE

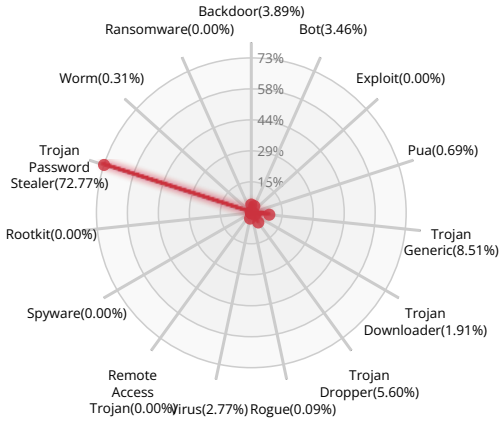
Xcitium Verdict Cloud Final Verdict

DETECTION SECTION

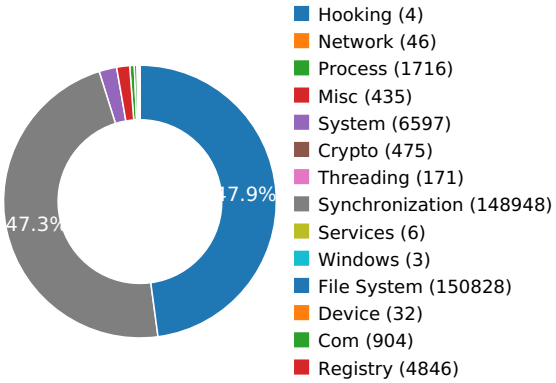


Verdict: Malware

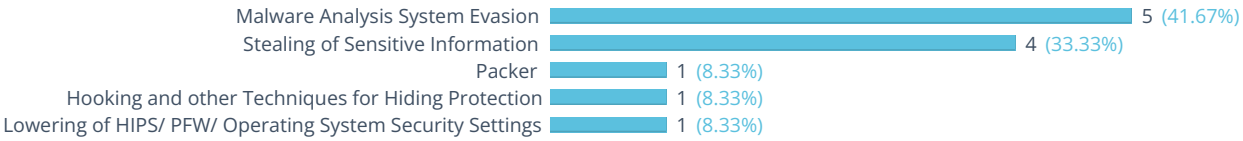
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

STEALING OF SENSITIVE INFORMATION

Collects information to fingerprint the system Show sources

Attempts to access Bitcoin/ALTCoin wallets Show sources

Steals private information from local Internet browsers Show sources

Harvests credentials from local FTP client softwares Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task. Show sources

Detects VirtualBox through the presence of a registry key Show sources

Checks the CPU name from registry, possibly for anti-virtualization Show sources

Checks the version of Bios, possibly for anti-virtualization Show sources

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

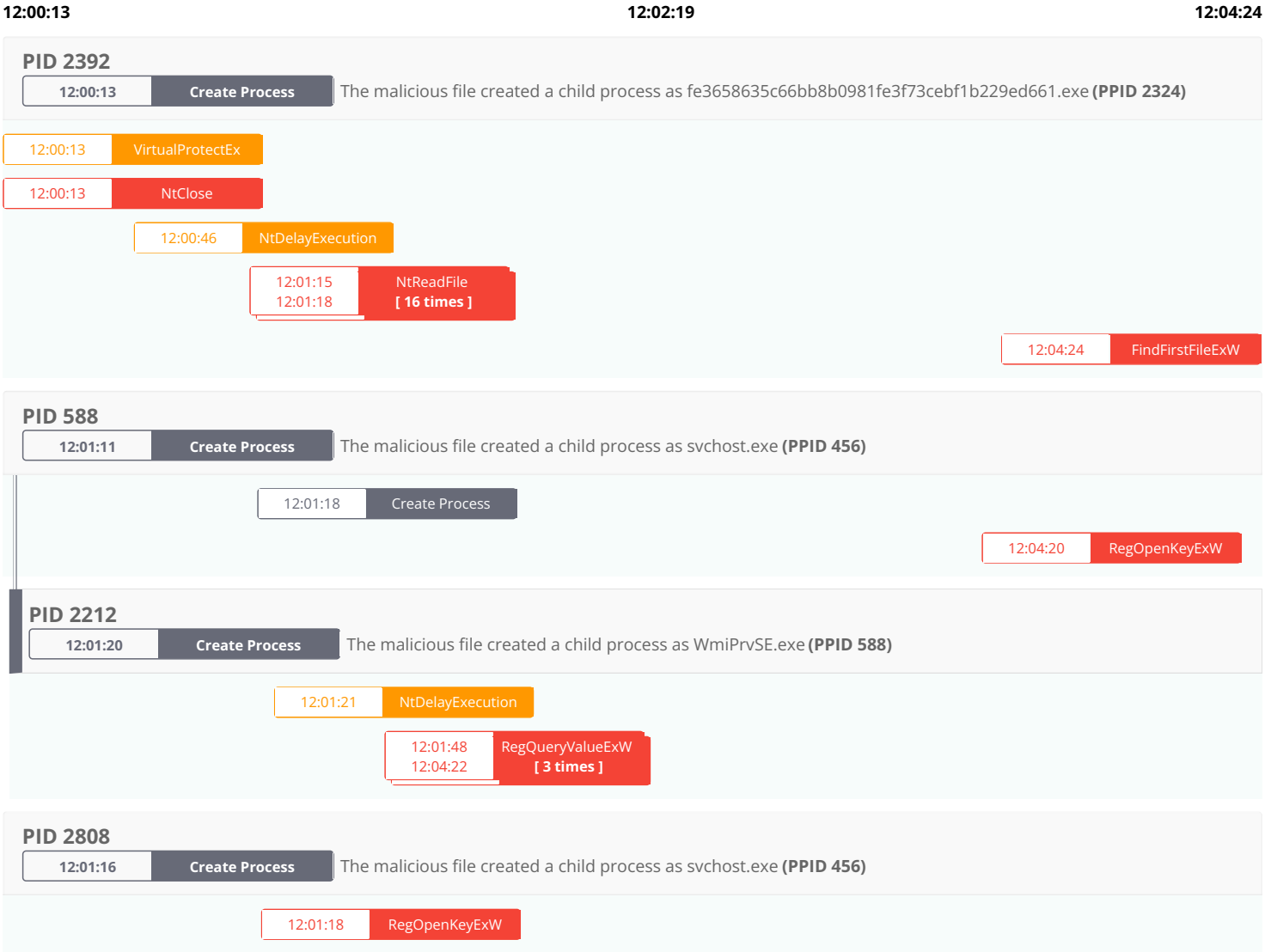
HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys Show sources

Behavior Graph



Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\msvcr100.dll
C:\Windows\System32\msvcr100.dll
C:\Windows\system\msvcr100.dll
C:\Windows\msvcr100.dll
C:\ProgramData\Oracle\Java\javapath\msvcr100.dll
C:\Windows\System32\wbem\msvcr100.dll
C:\Windows\System32\WindowsPowerShell\v1.0\msvcr100.dll
C:\Program Files\Microsoft Network Monitor 3\msvcr100.dll
C:\Program Files (x86)\Universal Extractor\msvcr100.dll
C:\Program Files (x86)\Universal Extractor\bin\msvcr100.dll
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\msvcr100.dll
C:\Python27\msvcr100.dll
C:\Python27\Scripts\msvcr100.dll
C:\tools\sysinternals\msvcr100.dll
C:\tools\msvcr100.dll
C:\tools\IDA_Pro_v6\python\msvcr100.dll
\Device\KsecDD
C:\Windows\System32\mscoree.dll.local
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework*
C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll
C:\Windows\Microsoft.NET\Framework\v1.0.3705\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v1.1.4322\clr.dll
C:\Windows\Microsoft.NET\Framework\v1.1.4322\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
C:\Users\user\AppData\Local\Temp\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\System32\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\system\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\ProgramData\Oracle\Java\javapath\api-ms-win-appmodel-runtime-l1-1-0.dll

C:\Windows\System32\wbem\api-ms-win-appmodel-runtime-l1-1-0.dll

C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-appmodel-runtime-l1-1-0.dll

C:\Program Files\Microsoft Network Monitor 3\api-ms-win-appmodel-runtime-l1-1-0.dll

C:\Program Files (x86)\Universal Extractor\api-ms-win-appmodel-runtime-l1-1-0.dll

C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-appmodel-runtime-l1-1-0.dll

C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-appmodel-runtime-l1-1-0.dll

C:\Python27\api-ms-win-appmodel-runtime-l1-1-0.dll

C:\Python27\Scripts\api-ms-win-appmodel-runtime-l1-1-0.dll

C:\tools\sysinternals\api-ms-win-appmodel-runtime-l1-1-0.dll

C:\tools\api-ms-win-appmodel-runtime-l1-1-0.dll

C:\tools\IDA_Pro_v6\python\api-ms-win-appmodel-runtime-l1-1-0.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSVCR120_CLR0400.dll

C:\Windows\System32\MSVCR120_CLR0400.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoree.dll

C:\Users\user\AppData\Local\Temp\fe3658635c66bb8b0981fe3f73cebf1b229ed661.exe.config

C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config

C:\Windows\Microsoft.NET\Framework\v4.0.30319\fusion.localgac

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

C:\Windows\Microsoft.Net\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib*

C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\225759bb87c854c0fff27b1d84858c21\mscorlib.ni.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\225759bb87c854c0fff27b1d84858c21\mscorlib.ni.dll.aux

C:\Windows\Microsoft.NET\Framework\v4.0.30319\ole32.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\OLEAUT32.dll

C:\Windows\assembly\pubpol20.dat

C:\Windows\assembly\GAC\PublisherPolicy.tme

C:\Windows\Microsoft.Net\assembly\GAC_MSIL_\v4.0_0.0.0.0__461d39c4a423da0b_.dll

C:\Windows\assembly\GAC_MSIL_\0.0.0.0__461d39c4a423da0b_.dll

C:\Windows\Microsoft.Net\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\oleaut32.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll

C:\Windows\Microsoft.Net\assembly\GAC_32\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.dll

C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms*

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\5aac750b35b27770dccb1a43f83cced7\System.Windows.Forms.ni.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\5aac750b35b27770dccb1a43f83cced7\System.Windows.Forms.ni.dll.aux

C:\Windows\Microsoft.Net\assembly\GAC_32\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System*
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\52cca48930e580e3189eac47158c20be\System.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\52cca48930e580e3189eac47158c20be\System.ni.dll.aux
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Configuration\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Configuration.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Xml\v4.0_4.0.0.0__b77a5c561934e089\System.Xml.dll
C:\Windows\Microsoft.Net\assembly\GAC_32\System.Drawing\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Drawing.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Drawing\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Drawing.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\CLRLoadLogDir
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\CacheLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DownloadCacheQuotaInKB
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\EnableLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LoggingLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\ForceLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogFailures
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\FileInUseRetryAttempts
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\FileInUseMillisecondsBetweenRetries
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\NGen\Policy\v4.0\OptimizeUsedBinaries
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\Latest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\index20
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\LegacyPolicyTimeStamp
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\AltJit
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
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\Time Zones\GTB Standard Time\TZI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\MUI_Display
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\MUI_Std
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\MUI_Dlt
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Client\InstallPath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\OnlyUseLatestCLR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Full\Release
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\AppCompat\RaiseDefaultAuthnLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\DefaultAccessPermission
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{00000134-0000-0000-C000-000000000046}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\NdrOleExtDLL
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\RemoteRpcDll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\67658C14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Hostname
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Domain
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9556DC99-828C-11CF-A37E-00AA003240C7}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\COM3\FinalizerActivityBypass
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{027947E1-D731-11CE-A357-000000000001}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\(Default)

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{1C1C45EE-4395-11D2-B60B-00104B703EFD}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{423EC01E-2E35-11D2-B604-00104B703EFD}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy\Enabled
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 024\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\ProductName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\CSDVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{1F87137D-0E7C-44D5-8C73-4EFFB68962F2}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{1F87137D-0E7C-44D5-8C73-4EFFB68962F2}\LocalServer32\LocalServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{1F87137D-0E7C-44D5-8C73-4EFFB68962F2}\LocalServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{1F87137D-0E7C-44D5-8C73-4EFFB68962F2}\LocalServer32\ServerExecutable
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{1F87137D-0E7C-44D5-8C73-4EFFB68962F2}\AppID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{1F87137D-0E7C-44D5-8C73-4EFFB68962F2}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{1F87137D-0E7C-44D5-8C73-4EFFB68962F2}\LocalService
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{1F87137D-0E7C-44D5-8C73-4EFFB68962F2}\DllSurrogate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{1F87137D-0E7C-44D5-8C73-4EFFB68962F2}\RunAs

MODIFIED FILES

\??\PIPE\samr
C:\Windows\sysnative\wbem\repository\WRITABLE.TST
C:\Windows\sysnative\wbem\repository\MAPPING1.MAP
C:\Windows\sysnative\wbem\repository\MAPPING2.MAP
C:\Windows\sysnative\wbem\repository\MAPPING3.MAP
C:\Windows\sysnative\wbem\repository\OBJECTS.DATA
C:\Windows\sysnative\wbem\repository\INDEX.BTR
\??\pipe\PIPE_EVENTROOT\CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM
\??\WMIDataDevice
\??\PIPE\wkssvc
\??\PIPE\srvsvc
\??\PHYSICALDRIVE0
\??\CDROM0
\??\PIPE\lsarpc

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.FlsFree
kernel32.dll.VirtualProtect
kernel32.dll.GlobalAlloc
kernel32.dll.GetLastError
kernel32.dll.Sleep
kernel32.dll.VirtualAlloc
kernel32.dll.CreateToolhelp32Snapshot
kernel32.dll.Module32First
kernel32.dll.CloseHandle
kernel32.dll.LoadLibraryA
kernel32.dll.VirtualFree
kernel32.dll.GetVersionExA
kernel32.dll.TerminateProcess
kernel32.dll.ExitProcess
kernel32.dll.SetErrorMode
kernel32.dll.RaiseException
kernel32.dll.MultiByteToWideChar
kernel32.dll.lstrlenA
kernel32.dll.InterlockedDecrement
kernel32.dll.GetProcAddress
kernel32.dll.FreeResource
kernel32.dll.SizeofResource
kernel32.dll.LockResource
kernel32.dll.LoadResource
kernel32.dll.FindResourceA
kernel32.dll.GetModuleHandleA
kernel32.dll.Module32Next
kernel32.dll.GetCurrentProcessId
kernel32.dll.SetEndOfFile
kernel32.dll.GetStringTypeW
kernel32.dll.GetStringTypeA

kernel32.dll.LCMapStringW
kernel32.dll.LCMapStringA
kernel32.dll.GetLocaleInfoA
kernel32.dll.HeapFree
kernel32.dll.GetProcessHeap
kernel32.dll.HeapAlloc
kernel32.dll.GetCommandLineA
kernel32.dll.HeapCreate
kernel32.dll.DeleteCriticalSection
kernel32.dll.LeaveCriticalSection
kernel32.dll.EnterCriticalSection
kernel32.dll.HeapReAlloc
kernel32.dll.HeapSize
kernel32.dll.GetCurrentProcess
kernel32.dll.UnhandledExceptionFilter
kernel32.dll.SetUnhandledExceptionFilter
kernel32.dll.IsDebuggerPresent
kernel32.dll.GetModuleHandleW
kernel32.dll.WriteFile
kernel32.dll.GetStdHandle
kernel32.dll.GetModuleFileNameA
kernel32.dll.WideCharToMultiByte
kernel32.dll.GetConsoleCP
kernel32.dll.GetConsoleMode
kernel32.dll.ReadFile
kernel32.dll.TlsGetValue
kernel32.dll.TlsAlloc
kernel32.dll.TlsSetValue
kernel32.dll.TlsFree
kernel32.dll.InterlockedIncrement
kernel32.dll.SetLastError
kernel32.dll.GetCurrentThreadId
kernel32.dll.FlushFileBuffers
kernel32.dll.SetFilePointer

kernel32.dll.SetHandleCount
kernel32.dll.GetFileType
kernel32.dll.GetStartupInfoA
kernel32.dll.RtlUnwind
kernel32.dll.FreeEnvironmentStringsA
kernel32.dll.GetEnvironmentStrings
kernel32.dll.FreeEnvironmentStringsW
kernel32.dll.GetEnvironmentStringsW

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\v4.0
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\CLRLoadLogDir
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_CURRENT_USER\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\fe3658635c66bb8b0981fe3f73cebf1b229ed661.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\CacheLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DownloadCacheQuotaInKB
HKEY_CURRENT_USER\Software\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\EnableLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LoggingLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\ForceLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogFailures
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\FileInUseRetryAttempts
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\FileInUseMillisecondsBetweenRetries
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\NGen\Policy\v4.0
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\NGen\Policy\v4.0\OptimizeUsedBinaries
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\Servicing
HKEY_LOCAL_MACHINE\Software\Microsoft\StrongName
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\Latest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\index20
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\LegacyPolicyTimeStamp
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.0.0.___461d39c4a423da0b
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.0.0.___461d39c4a423da0b
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\AltJit
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Windows.Forms__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Windows.Forms__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Configuration__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Configuration__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Xml__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Xml__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Drawing__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Drawing__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Security__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Security__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.Accessibility__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.Accessibility__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Core__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Core__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Deployment__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Deployment__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Runtime.Serialization.Formatters.Soap__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Runtime.Serialization.Formatters.Soap__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\APTCA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.1.9.Tombolas__461d39c4a423da0b

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.1.9.Tombolas__461d39c4a423da0b
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\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\Time Zones\GTB Standard Time
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\TZI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\Dynamic DST
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\MUI_Display
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\MUI_Std
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\MUI_Dlt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.PresentationFramework__31bf3856ad364e35
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.PresentationFramework__31bf3856ad364e35

READ FILES

\Device\KsecDD
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
C:\Windows\System32\MSVCR120_CLR0400.dll
C:\Users\user\AppData\Local\Temp\fe3658635c66bb8b0981fe3f73cebf1b229ed661.exe.config
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\225759bb87c854c0fff27b1d84858c21\mscorlib.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\225759bb87c854c0fff27b1d84858c21\mscorlib.ni.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\5aac750b35b27770dccb1a43f83cced7\System.Windows.Forms.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\52cca48930e580e3189eac47158c20be\System.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\52cca48930e580e3189eac47158c20be\System.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\646b4b01cb29986f8e076aa65c9e9753\System.Drawing.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\646b4b01cb29986f8e076aa65c9e9753\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\5aac750b35b27770dccb1a43f83cced7\System.Windows.Forms.ni.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorrc.dll

C:\Windows\System32\tzres.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\nlssorting.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\SortDefault.nlp

C:\Windows\System32\en-US\tzres.dll.mui

C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\da36abbea6ef456f432434d4d8d835c1\PresentationFramework.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\32512bd09e2231f6eebb15fc17e3ad79\WindowsBase.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\55560c2014611e9119f99923c9ebdeef\System.Core.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\55560c2014611e9119f99923c9ebdeef\System.Core.ni.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\32512bd09e2231f6eebb15fc17e3ad79\WindowsBase.ni.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\416ba33cb980d07643e82c4c45bd5786\PresentationCore.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\416ba33cb980d07643e82c4c45bd5786\PresentationCore.ni.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\da36abbea6ef456f432434d4d8d835c1\PresentationFramework.ni.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\WPF\wpfgfx_v0400.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\WPF\PresentationNative_v0400.dll

C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.ServiceModel\v4.0_4.0.0.0__b77a5c561934e089\System.ServiceModel.dll

C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Runtime.Serialization\v4.0_4.0.0.0__b77a5c561934e089\System.Runtime.Serialization.dll

C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.IdentityModel\v4.0_4.0.0.0__b77a5c561934e089\System.IdentityModel.dll

C:\Windows\Microsoft.Net\assembly\GAC_MSIL\SMDiagnostics\v4.0_4.0.0.0__b77a5c561934e089\SMDiagnostics.dll

C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.ServiceModel.Internals\v4.0_4.0.0.0__31bf3856ad364e35\System.ServiceModel.Internals.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\d86b080a37c60a872c82b912a2a63dac\System.Xml.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\d86b080a37c60a872c82b912a2a63dac\System.Xml.ni.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\46957030830964165644b52b0696c5d9\System.Configuration.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\46957030830964165644b52b0696c5d9\System.Configuration.ni.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transactions\e7044d177c8e852b85908d2702898ec8\System.Transactions.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transactions\e7044d177c8e852b85908d2702898ec8\System.Transactions.ni.dll

C:\Windows\Microsoft.Net\assembly\GAC_32\System.Transactions\v4.0_4.0.0.0__b77a5c561934e089\System.Transactions.dll

C:\Windows\Microsoft.Net\assembly\GAC_32\System.Transactions\v4.0_4.0.0.0__b77a5c561934e089\System.Transactions.dll.config

C:\Windows\Microsoft.Net\assembly\GAC_MSIL\Microsoft.CSharp\v4.0_4.0.0.0__b03f5f7f11d50a3a\Microsoft.CSharp.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\4dfa27fdd6a4cce26f99585e1c744f9b\System.Management.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\4dfa27fdd6a4cce26f99585e1c744f9b\System.Management.ni.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\wminet_utils.dll

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State

C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Web.Extensions\v4.0_4.0.0.0__31bf3856ad364e35\System.Web.Extensions.dll

C:\Windows\Microsoft.Net\assembly\GAC_32\System.Web\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Web.dll

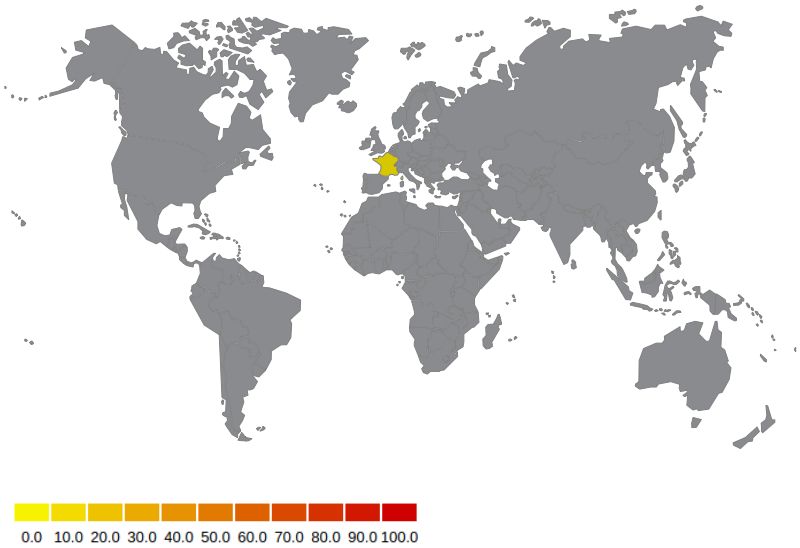
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Security\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Security.dll
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Windows\sysnative\wbem\WmiPrvSE.exe
C:\Windows\inf\disk.PNF
C:\Windows\inf\oem16.PNF
\??\PIPE\samr
C:\Windows\sysnative\wbem\repository\MAPPING1.MAP
C:\Windows\sysnative\wbem\repository\MAPPING2.MAP
C:\Windows\sysnative\wbem\repository\MAPPING3.MAP
C:\Windows\sysnative\wbem\repository\OBJECTS.DATA
C:\Windows\sysnative\wbem\repository\INDEX.BTR
\??\pipe\PIPE_EVENTROOT\CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM
\??\ide#diskvbox_harddisk_____1.0____#5&33d1638a&0&0.0.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
\??\WMIDataDevice
C:\Windows\Branding\Basebrd\basebrd.dll
C:
C:\Windows\sysnative\tzres.dll

MODIFIED REGISTRY KEYS

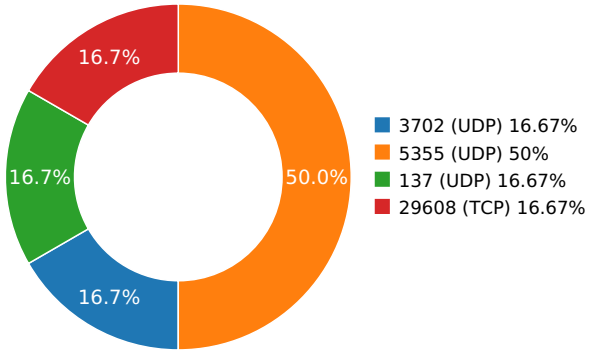
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Transports\Decoupled\Server
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\CreationTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\MarshaledProxy
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\ProcessIdentifier
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ConfigValueEssNeedsLoading
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\List of event-active namespaces

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	178.32.90.250	France	16276	Failover Ips	Malware Process

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
38.8148019314	Sandbox	178.32.90.250	29608

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.18565797806	Sandbox	224.0.0.252	5355
3.18847298622	Sandbox	192.168.56.255	137
3.23207592964	Sandbox	224.0.0.252	5355
3.25781702995	Sandbox	239.255.255.250	3702
5.75020289421	Sandbox	224.0.0.252	5355

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	fe3658635c66bb8b0981fe3f73cebf1b229ed661
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	fe3658635c66bb8b0981fe3f73cebf1b229ed661
MD5:	a48de889c19197426214da54922eb7ad
First Seen Date:	2023-07-20 10:16:32.895832 (4 days ago)
Number Of Clients Seen:	4
Last Analysis Date:	2023-07-20 10:39:04.237325 (4 days ago)
Human Expert Analysis Date:	2023-07-20 18:47:44.243530 (4 days ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[{u'Path': u'C:\\lepofutu\\kafi\\90_kexof.pdb\x00', u'GUID': u'{51a7bed9-7f7e-47cc-a7f3-5a4b36c4c767}', u'timestamp': u'2023-07-14 02:29:38'}]
Number Of Sections	4
Trid	[[76.4, u'Win64 Executable (generic)'], [12.4, u'Win32 Executable (generic)'], [5.5, u'Generic Win/DOS Executable'], [5.5, u'DOS Executable Generic']]
Compilation Time Stamp	0x637C6365 [Tue Nov 22 05:51:33 2022 UTC]
LegalCopyright	Copyright (C) 2023, historic
ProductName	Fruits
ProductsVersion	32.64.57.24
ProductionVersion	75.19.17.96
FileDescription	Underweather
Translation	0x07fd 0x0855
Entry Point	0x405de7 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	405504
Ssdeep	6144:FdJL5aCNSwXadmlzRO3YUMmJxqD54zt2ySqOOS:7J1ahld8RUYUzED5It2POS
Sha256	f4fed6410af40a0441fd09c9f8d2b203938d46b8ae18dd75f6ea78ac9f675a2b
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/f/e/3/6/fe3658635c66bb8b0981fe3f73cebf1b229ed661', u'EXE:ProductName': u'Fruits', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2023:07:20 10:15:50+00:00', u'EXE:InitializedDataSize': 33525760, u'File:FileModifyDate': u'2023:07:20 10:15:49+00:00', u'EXE:ProductsVersion': u'32.64.57.24', u'EXE:ProductionVersion': u'75.19.17.96', u'EXE:FileVersionNumber': u'74.0.0.0', u'File:FileSize': u'396 kB', u'EXE:CharacterSet': u'Unknown (31F2)', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Unknown (0x20761)', u'EXE:ObjectFileType': u'Unknown', u'File:FileType': u'Win32 EXE', u'EXE:UninitializedDataSize': 0, u'File:FileName': u'fe3658635c66bb8b0981fe3f73cebf1b229ed661', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 5.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2022:11:22 05:51:33+00:00', u'EXE:FileFlagsMask': u'0x141a', u'EXE:LegalCopyright': u'Copyright (C) 2023, historic', u'EXE:LinkerVersion': 9.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/f/e/3/6', u'EXE:FileDescription': u'Underweather', u'EXE:EntryPoint': u'0x5de7', u'EXE:SubsystemVersion': 5.0, u'EXE:CodeSize': 230400, u'File:FileInodeChangeDate': u'2023:07:20 10:15:49+00:00', u'EXE:LanguageCode': u'Faeroese', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'36.0.0.0'}]
Mime Type	application/x-dosexec
Imphash	01c4ee1c294ad77d8fcb236b1ae3a868

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x3825c	0x38400	7.79393372885	7d149c1a91239df913ab218c4ef371d8
.data	0x3a000	0x1fd001c	0x1a00	2.11885652094	9084ffb95c1be5496dffe45ba4457e77
.rsrc	0x200b000	0x1faf0	0x1fc00	4.08000889801	e846b6b5ad2124015465e85691602b0e
.reloc	0x202b000	0x9168	0x9200	0.978377933854	aad80466572b44e5319dff91c83817a6

PE Imports

- KERNEL32.dll
  - lstrlenA
  - GetConsoleAliasesLengthW
  - EnumDateFormatsExW
  - FindResourceW
  - GlobalAddAtomA
  - EnumCalendarInfoW
  - _lwrite
  - AddConsoleAliasW
  - GetComputerNameW
  - GetTickCount
  - GetConsoleAliasesA
  - GetWindowsDirectoryA
  - WriteFile
  - GlobalAlloc
  - LoadLibraryW
  - ReadConsoleInputA
  - FreeConsole
  - EnumSystemCodePagesA
  - FindNextVolumeW
  - GetCompressedFileSizeA
  - SetThreadPriority
  - DisconnectNamedPipe
  - GetConsoleAliasesW
  - CreateMutexW
  - GetProfileIntA
  - OpenMutexW
  - SetLastError
  - lstrcmpiA
  - GetProcAddress
  - VirtualAlloc
  - SearchPathA
  - LoadLibraryA
  - SetCurrentDirectoryW
  - GetOEMCP
  - SetLocaleInfoW
  - CreateMutexA
  - FatalAppExitA
  - ScrollConsoleScreenBufferA
  - SetProcessShutdownParameters
  - _lopen
  - OpenSemaphoreW
  - SetFileShortNameA
  - AddConsoleAliasA
  - LocalFileTimeToFileTime
  - CreateFileA
  - CloseHandle
  - WriteConsoleW
  - InterlockedExchange
  - GetDateFormatW
  - InterlockedIncrement
  - InterlockedDecrement
  - Sleep
  - InitializeCriticalSection
  - DeleteCriticalSection
  - EnterCriticalSection
  - LeaveCriticalSection
  - UnhandledExceptionFilter
  - SetUnhandledExceptionFilter
  - GetLastError
  - HeapFree

    - MultiByteToWideChar
    - GetStartupInfoW
    - RtlUnwind
    - RaiseException
    - GetModuleHandleW
    - ExitProcess
    - GetStdHandle
    - GetModuleFileNameA
    - HeapAlloc
    - HeapCreate
    - VirtualFree
    - HeapReAlloc
    - SetHandleCount
    - GetFileType
    - GetStartupInfoA
    - TerminateProcess
    - GetCurrentProcess
    - IsDebuggerPresent
    - GetCPInfo
    - GetACP
    - IsValidCodePage
    - TlsGetValue
    - TlsAlloc
    - TlsSetValue
    - TlsFree
    - GetCurrentThreadId
    - GetModuleFileNameW
    - FreeEnvironmentStringsW
    - GetEnvironmentStringsW
    - GetCommandLineW
    - QueryPerformanceCounter
    - GetCurrentProcessId
    - GetSystemTimeAsFileTime
    - HeapSize
    - GetLocaleInfoA
    - GetStringTypeA
    - GetStringTypeW
    - InitializeCriticalSectionAndSpinCount
    - SetFilePointer
    - WideCharToMultiByte
    - GetConsoleCP
    - GetConsoleMode
    - LCMapStringA
    - LCMapStringW
    - FlushFileBuffers
    - SetStdHandle
    - WriteConsoleA
    - GetConsoleOutputCP
- USER32.dll
    - DdeQueryStringW
    - CharUpperBuffA
    - LoadMenuW
    - CharLowerBuffW
- ADVAPI32.dll
    - InitializeAcl

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 33726248, u'sha256': u'609cf0e1c5d2f8c59ce55228574bd35efef29d9ea018a50a9bc73703d4170006', u'type': u'data', u'size': 304}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 33726552, u'sha256': u'67ceff3facc1ae98c4212a57be34fd73f7ac41d47c65002d6b77f7a3f3d33144', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 176}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33601936, u'sha256': u'a666afd3e4f2ae14376d1aaf6ebb0363e4cb3fcf3e074bb917165000dffc751c', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33605688, u'sha256': u'311fe735d4737b0fb08580124d9ae3aad8ce3814db9c2a735691b93b4680c4df', u'type': u'data', u'size': 2216}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33607904, u'sha256': u'748be7e442b638cc22722acf1d312e6143702007bc128ad08aa546f850052f8b', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 9640}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33617544, u'sha256': u'632f3adf7b5ef345ecdd2057c6b9d8d940cf4fb812d3a74cab829caca25087b4', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33621808, u'sha256': u'f0a50e6419f34115e8bc5e9e630be26da9cb6ef143a341907645dca29044cd65', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33623016, u'sha256':

u'e4a2f7038c2ceca105d45e0c56251421b91530f2fe7c6c798b5d380abe640d89', u'type': u'data', u'size': 3752}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33626768, u'sha256': u'dfc34afdf97c4ecc41842947381804a3ebc50fe368f6946e2fa97bbc0a8684ff', u'type': u'data', u'size': 2216}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33628984, u'sha256': u'de3e53e3244fdfbaab09bd199d42fde1c978ff74554817f40bb958423b49a6b9', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33630368, u'sha256': u'bf71c5d6d306e21ea3949c1fbb7d39cb156bf2e15e2971524d0b4eef0b929543', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33640008, u'sha256': u'4225a26fe42ddd8381d9feb12427f89fbb35d914db5d12ffa75c34b0e7fb6aad', u'type': u'data', u'size': 4264}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33644272, u'sha256': u'f47568d1e910f8982cbb5916d7d722beb2063c87218d36a19ffab59464a3b0e3', u'type': u'data', u'size': 2440}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33646712, u'sha256': u'1f230a0d458a0ea150ce020579c65e056d318e876ee7f25d22323dcaad9ce985', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33647944, u'sha256': u'693d8d82a0da488903270aee555f801f0d549eedef17188dbf9a9dd0d442097c', u'type': u'data', u'size': 3752}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33651696, u'sha256': u'0dcdbe8a931fffa860c73ea3602eddc70f2be4247e05abb23a81cef41f8290c4', u'type': u'dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 8486783, next used block 8487041', u'size': 2216}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33653912, u'sha256': u'c6aee3fb118b359f7f3e6937de46e5e3c7f9c377fc9078c2021be77e4da23099', u'type': u'data', u'size': 1736}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33655648, u'sha256': u'7aa39916bde3ef77b5422355a3852e8d43ee3c7e1efa5ffa66734814c36b3ffe', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33657032, u'sha256': u'c3fb7b29234e19d881f53d5752d10215314475f9e4e63fe1c4b96be17d3754fb', u'type': u'dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0', u'size': 9640}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33666672, u'sha256': u'2a0bd0f482e442287bc9e0068b1e25b7f70f500e4a3207d8687cdfaa6a6f0609', u'type': u'dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 2139127680, next used block 2172616577', u'size': 4264}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33670936, u'sha256': u'14f307f3bebe7f8f19c71f12806d92811b7ebcc4e33ac8c9b058e050da2f2eb5', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33673376, u'sha256': u'0c5d1617edfd3f3163334bceb32ca0dddc4efef7091455ac4a77c1c56b4c9ef7', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33674624, u'sha256': u'3656b29897cb3d5403daf139d2fc89b54ebf3901ec58cba39bb74d9c8f3350f0', u'type': u'data', u'size': 3752}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33678376, u'sha256': u'7bc7052d2337b334c3cec97b08018acd5662362199c16d4ec3b6967d697b9689', u'type': u'data', u'size': 2216}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33680592, u'sha256': u'6c2111f65fc89a00fed15352455f525a87be49ad76cf2fcf32cd752c366aab97', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33681976, u'sha256': u'2e7c06e8886b5776c234abc985be512319c799e512ee014642b33f9b4dba7527', u'type': u'data', u'size': 9640}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33691616, u'sha256': u'75d7dc4cc8d39efc920917c72b1009bc7e3f81509c8d3446f018d07ec2313139', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33695880, u'sha256': u'05f7f5966632bf7e5a61e7764d5bf94ad899d931a55ed28debb9c8428f4d08a9', u'type': u'data', u'size': 2440}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33698320, u'sha256': u'78abf7426193331d5fc244a03b9d59ecdf18807ae01dd80bba7c505f6248817b', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33699552, u'sha256': u'ef024e149e1f020a36c94e15dd96cebde21d73b15a78327e0bc432614e3971ba', u'type': u'data', u'size': 3752}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33703304, u'sha256': u'50bd97c2c17ac945cfeb0140cb7d297a4ef96febc4c63fde17c747ef9461509b', u'type': u'data', u'size': 2216}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33705520, u'sha256': u'a234da42fa7c694a3ed14d0c734d006be412cb6be46f73e101240c69307a6173', u'type': u'data', u'size': 1736}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33707256, u'sha256': u'fd5e468da0d84731ffc7e8eedf39191bd5606edd2ac34b3537acee2458f8855d', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33708640, u'sha256': u'761cc770ebbe93c41a084a1ef12d3eda4f96b780fe9f39a62712cc15e16b6053', u'type': u'data', u'size': 9640}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33718280, u'sha256': u'3b01425f8a888854f8a7934b3169a8e8c76a04ca773eb317e9da275ee370bfe3', u'type': u'data', u'size': 4264}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33722544, u'sha256': u'6da3af8f955f48528555c713ce8c2834b2a8d5130c456d507b7a673df3a79ff1', u'type': u'data', u'size': 2440}


{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_ICON', u'offset': 33724984, u'sha256': u'31f3496f7b71ae5fbbd0af662ce7268e8e6b7127709ed7bb55563da2c56c7443', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}


{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 33727336, u'sha256': u'a9566e7e84a8a200f6b9d080f3d0c3932ef4d050644cc5d06bc9056ce4bab62a', u'type': u'data', u'size': 1372}


{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 33728712, u'sha256': u'23ed4fe69304bca2cd0c770baf53759f689c05d0b1f455794210d9ed927ef062', u'type': u'data', u'size': 546}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 33726728, u'sha256': u'be5db25a165b649701f88c017e632e6733e43938e1342e3a4d885a471d42c618', u'type': u'MS Windows icon resource - 2 icons, 32x32, 2 colors', u'size': 34}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_GROUP_ICON', u'offset': 33622936, u'sha256': u'5daa005129f6706482a1ce299959e546bc0525594a44f2e4c14f99bf5dde9ac3', u'type': u'MS Windows icon resource - 5 icons, 48x48', u'size': 76}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_GROUP_ICON', u'offset': 33647840, u'sha256': u'175c44cd427ffa52ec94040b15fee5c8af481e715ab585dbfa4938b18d6efd9b', u'type': u'MS Windows icon resource - 7 icons, 48x48', u'size': 104}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_GROUP_ICON', u'offset': 33674504, u'sha256': u'f021825f19bdd266589a740e022304a9d050670d15390948bd034503bf4e6e26', u'type': u'MS Windows icon resource - 8 icons, 48x48', u'size': 118}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_GROUP_ICON', u'offset': 33726112, u'sha256': u'9b3b1518bf5f1aafc04111fac5e8528214768123db6029d013eb17a922fc6f7b', u'type': u'MS Windows icon resource - 8 icons, 48x48', u'size': 118}

{u'lang': u'LANG_PORTUGUESE', u'name': u'RT_GROUP_ICON', u'offset': 33699448, u'sha256': u'b1fe53b069e5fc407b674159dd4b277cb60093f857a7294e3d4571134e34a583', u'type': u'MS Windows icon resource - 7 icons, 48x48', u'size': 104}

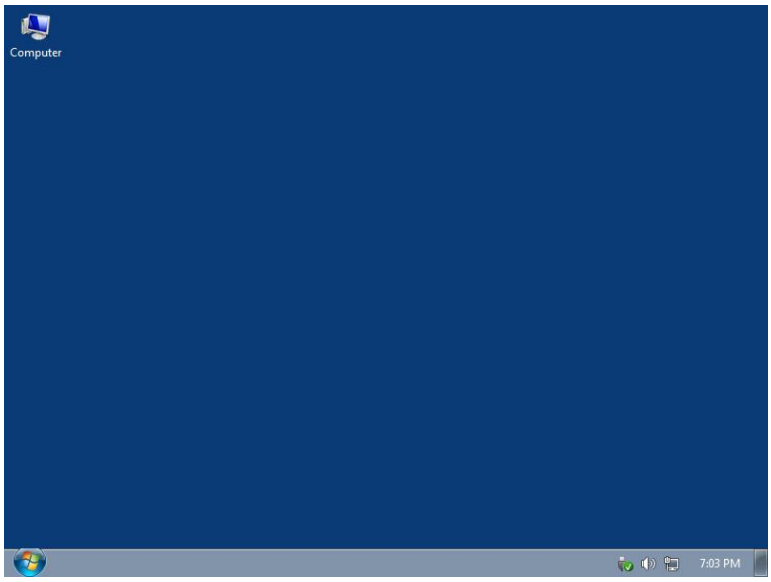
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 33726768, u'sha256': u'5d0ee16eb1df426580b6f10abad19b0a8b9bc0fde94b1da3c44b4aa8b785eb0a', u'type': u'data', u'size': 564}

{u'lang': u'LANG_NEUTRAL', u'name': u'241', u'offset': 33726232, u'sha256': u'2aae662c2afa7f5a59bfcae85b9dd1b56003e39da081ed0921c06d7deeadf12b', u'type': u'data', u'size': 10}

CERTIFICATE VALIDATION

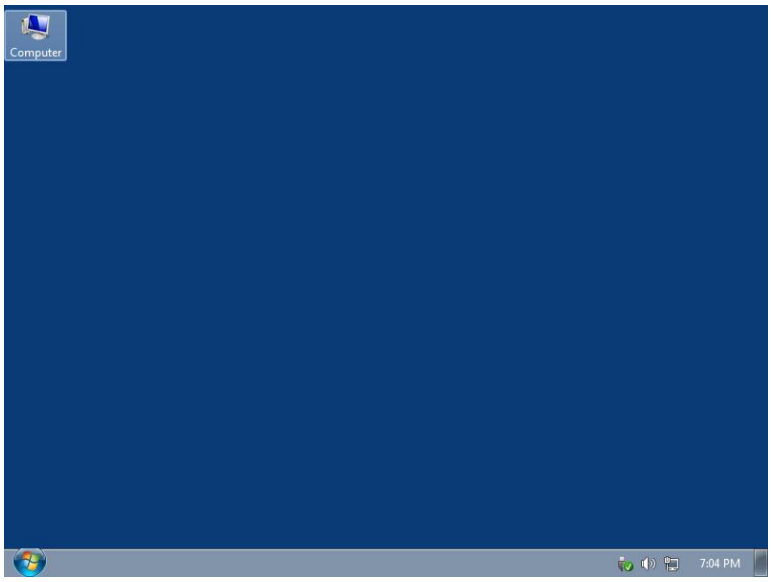
- Certificate Validation is not Applicable ?

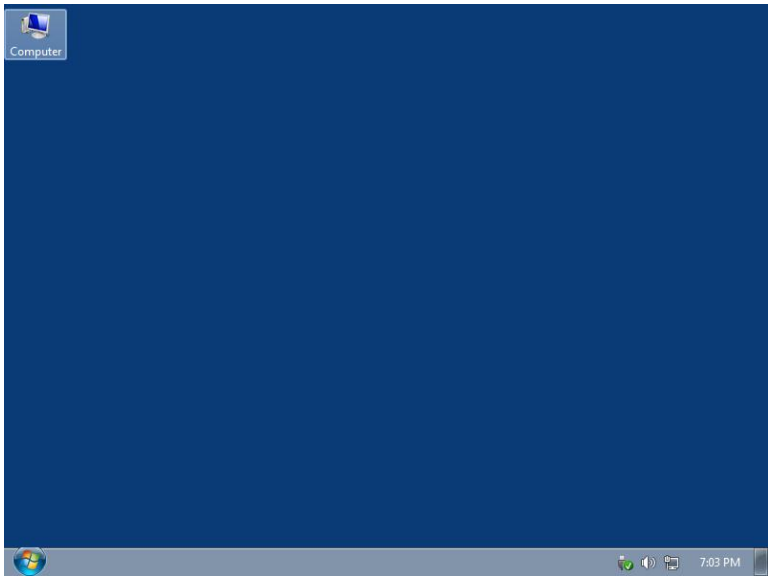
SCREENSHOTS


Computer
7:03 PM


Computer
7:02 PM


Computer
7:00 PM


Computer
7:04 PM


Computer
7:03 PM