Summary

File Name: Transfer.exe

File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

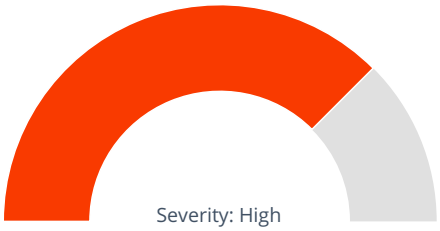
SHA1: e38a9f88f272ad1c712d369384f5fb9770b804ca

MD5: 461256eec678cf899ac154263c2d8c4d

MALWARE

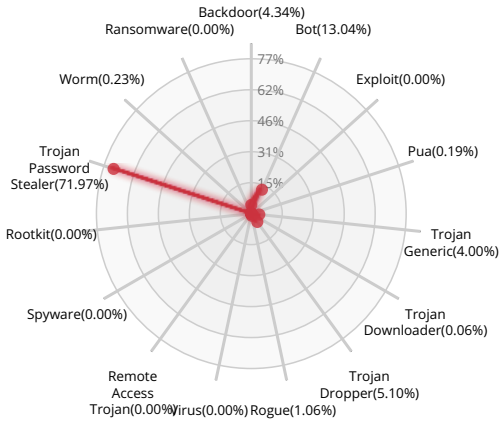
Valkyrie Final Verdict

DETECTION SECTION

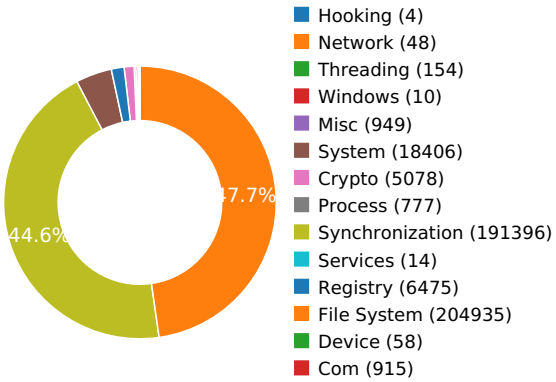


Verdict: Malware

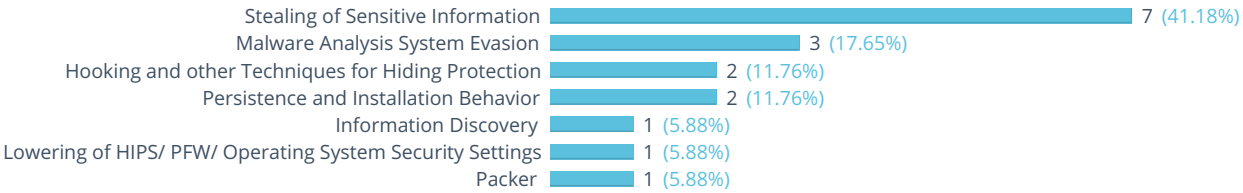
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Attempts to remove evidence of file being downloaded from the Internet	Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys	

PACKER

The binary likely contains encrypted or compressed data.	Show sources

STEALING OF SENSITIVE INFORMATION

Looks up the external IP address	Show sources
Collects information to fingerprint the system	
Sniffs keystrokes	Show sources
Steals private information from local Internet browsers	Show sources
Harvests information related to installed instant messenger clients	Show sources
Harvests credentials from local FTP client softwares	Show sources
Harvests information related to installed mail clients	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	
Executed a process and injected code into it, probably while unpacking	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup	Show sources
Creates a copy of itself	Show sources

MALWARE ANALYSIS SYSTEM EVASION

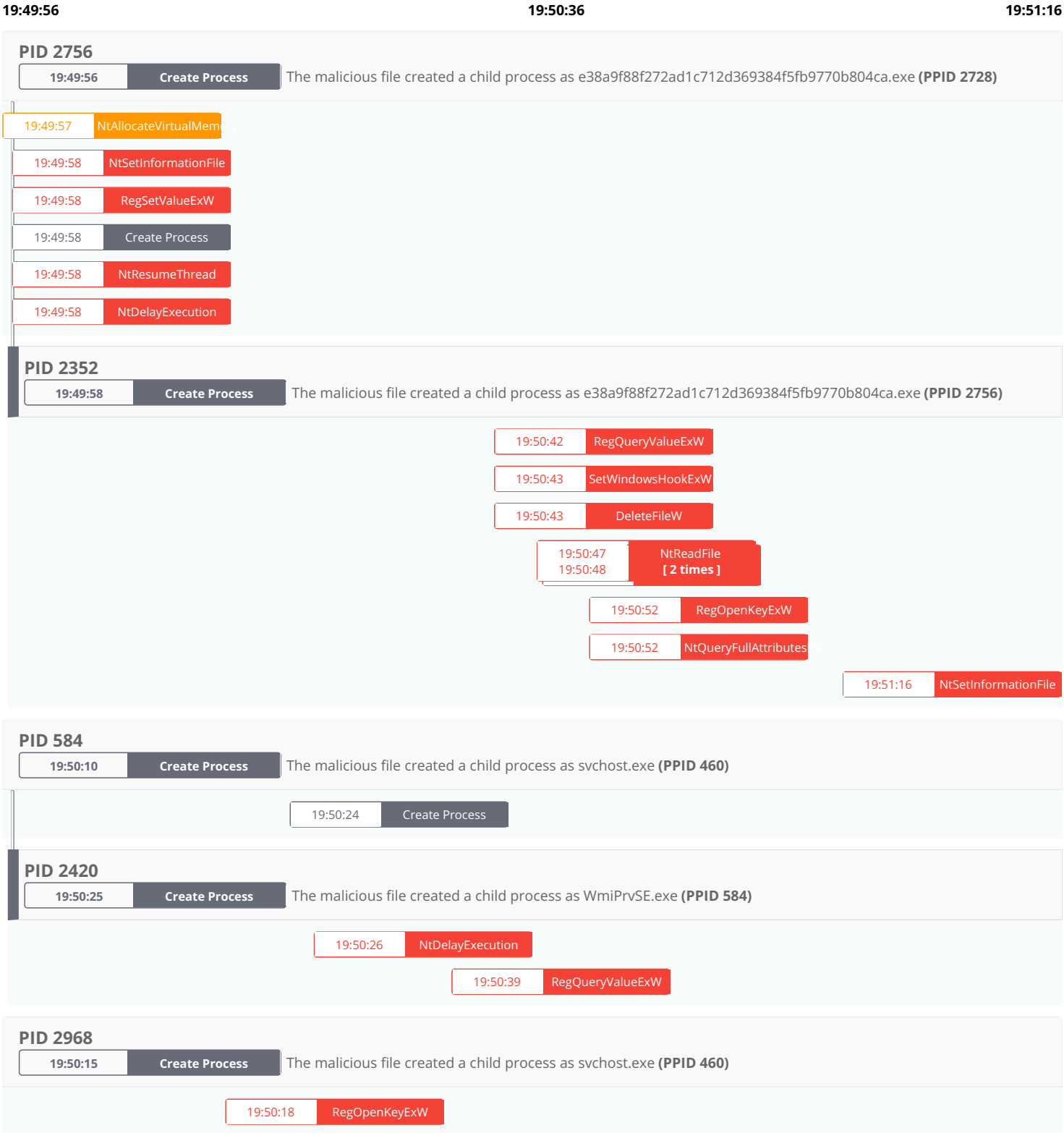
Checks the CPU name from registry, possibly for anti-virtualization

A process attempted to delay the analysis task by a long amount of time. Show sources

Creates a hidden or system file Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

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\e38a9f88f272ad1c712d369384f5fb9770b804ca.exe.config
C:\Users\user\AppData\Local\Temp\e38a9f88f272ad1c712d369384f5fb9770b804ca.exe
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:\Users\user\AppData\Local\Temp\e38a9f88f272ad1c712d369384f5fb9770b804ca.exe.Local\
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll
C:\Windows

C:\Windows\winsxs
C:\Windows\Microsoft.NET\Framework\v4.0.30319
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\fusion.localgac
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_32\index126.dat
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\62a0b3e4b40ec0e8c5cfaa0c8848e64a\mscorlib.ni.dll
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.INI
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ole32.dll
\Device\KsecDD
C:\Windows\System32\l_intl.nls
C:\Users\user\AppData\Local\Temp\e38a9f88f272ad1c712d369384f5fb9770b804ca.INI
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\GAC\PublisherPolicy.tme
C:\Windows\assembly\NativeImages_v2.0.50727_32\System\9e0a3b9b9f457233a335d7fba8f95419\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\08d608378aa405adc844f3cf36974b8c\Microsoft.VisualBasic.ni.dll
C:\Windows\assembly\GAC_MSIL\Microsoft.VisualBasic\8.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.INI
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.INI
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\dbfe8642a8ed7b2b103ad28e0c96418a\System.Drawing.ni.dll
C:\Windows\assembly\GAC_MSIL\System.Drawing\2.0.0.0__b03f5f7f11d50a3a\System.Drawing.INI
C:\Windows\Globalization\en-us.nlp
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Users\user\AppData\Local\Temp\en-US\kosi.resources.dll

C:\Users\user\AppData\Local\Temp\en-US\kosi.resources\kosi.resources.dll
C:\Users\user\AppData\Local\Temp\en-US\kosi.resources.exe
C:\Users\user\AppData\Local\Temp\en-US\kosi.resources\kosi.resources.exe
C:\Windows\Microsoft.NET\Framework\v2.0.50727\Culture.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\en-US\mscorrc.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\en-US\mscorrc.dll.DLL
C:\Windows\Microsoft.NET\Framework\v2.0.50727\en\mscorrc.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\en\mscorrc.dll.DLL
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorrc.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\CLRLoadLogDir
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\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStart
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStartAtJit
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\VersioningLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126\NIUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126\ILUsageMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigString

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MVID

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\EvalationData

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\Status

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ILDependencies

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\NIDependencies

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MissingDependencies

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Status

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Modules

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\SIG

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\LastModTime

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\mscorlib,2.0.0.0,,b77a5c561934e089,x86

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\NativeImagesIndex\v2.0.50727_32\NI\1c22df2f\4f99a7c9\2e\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\1c22df2f\4f99a7c9\2e\ConfigMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\1c22df2f\4f99a7c9\2e\ConfigString

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\1c22df2f\4f99a7c9\2e\MVID

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\1c22df2f\4f99a7c9\2e\EvalationData

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\1c22df2f\4f99a7c9\2e\Status

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\1c22df2f\4f99a7c9\2e\ILDependencies

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\1c22df2f\4f99a7c9\2e\NIDependencies

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\1c22df2f\4f99a7c9\2e\MissingDependencies

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\c991064\2bd33e1c\79\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\c991064\2bd33e1c\79\Status

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\c991064\2bd33e1c\79\Modules

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\c991064\2bd33e1c\79\SIG

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\c991064\2bd33e1c\79\LastModTime

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\6dc7d4c0\a5cd4db\7e\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\6dc7d4c0\a5cd4db\7e\Status

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\6dc7d4c0\a5cd4db\7e\Modules

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\6dc7d4c0\a5cd4db\7e\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\6dc7d4c0\a5cd4db\7e\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\3ced59c5\1b2590b1\7c\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\3ced59c5\1b2590b1\7c\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\3ced59c5\1b2590b1\7c\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\3ced59c5\1b2590b1\7c\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\3ced59c5\1b2590b1\7c\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\f6e8397\46ad0879\6f\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\f6e8397\46ad0879\6f\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\f6e8397\46ad0879\6f\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\f6e8397\46ad0879\6f\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\f6e8397\46ad0879\6f\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\2b1a4e4\38a3212c\44\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\2b1a4e4\38a3212c\44\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\2b1a4e4\38a3212c\44\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\2b1a4e4\38a3212c\44\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\2b1a4e4\38a3212c\44\LastModTime

MODIFIED FILES

C:\Users\user\AppData\Roaming\Java\JavaUpdtr.exe
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Users\user\AppData\Roaming\ScreenShot\screen.jpeg
\??\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

RESOLVED APIS

advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
advapi32.dll.RegEnumKeyExW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
kernel32.dll.FlsAlloc
kernel32.dll.FlsFree
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.CreateEventExW
kernel32.dll.CreateSemaphoreExW
kernel32.dll.SetThreadStackGuarantee
kernel32.dll.CreateThreadpoolTimer
kernel32.dll.SetThreadpoolTimer
kernel32.dll.WaitForThreadpoolTimerCallbacks
kernel32.dll.CloseThreadpoolTimer
kernel32.dll.CreateThreadpoolWait
kernel32.dll.SetThreadpoolWait
kernel32.dll.CloseThreadpoolWait
kernel32.dll.FlushProcessWriteBuffers
kernel32.dll.FreeLibraryWhenCallbackReturns
kernel32.dll.GetCurrentProcessorNumber
kernel32.dll.GetLogicalProcessorInformation
kernel32.dll.CreateSymbolicLinkW
kernel32.dll.EnumSystemLocalesEx
kernel32.dll.CompareStringEx
kernel32.dll.GetDateFormatEx
kernel32.dll.GetLocaleInfoEx
kernel32.dll.GetTimeFormatEx
kernel32.dll.GetUserDefaultLocaleName

kernel32.dll.IsValidLocaleName
kernel32.dll.LCMapStringEx
kernel32.dll.GetTickCount64
advapi32.dll.EventRegister
mscoree.dll.#142
mscoreei.dll.RegisterShimImplCallback
mscoreei.dll.OnShimDllMainCalled
mscoreei.dll._CorExeMain
shlwapi.dll.UrlIsW
version.dll.GetFileVersionInfoSizeW
version.dll.GetFileVersionInfoW
version.dll.VerQueryValueW
kernel32.dll.InitializeCriticalSectionAndSpinCount
kernel32.dll.IsProcessorFeaturePresent
msvcrt.dll._set_error_mode
msvcrt.dll.?set_terminate@@YAP6AXXZP6AXXZ@Z
kernel32.dll.FindActCtxSectionStringW
kernel32.dll.GetSystemWindowsDirectoryW
mscoree.dll.GetProcessExecutableHeap
mscoreei.dll.GetProcessExecutableHeap
mscorwks.dll._CorExeMain
mscorwks.dll.GetCLRFunction
advapi32.dll.RegisterTraceGuidsW
advapi32.dll.UnregisterTraceGuids
advapi32.dll.GetTraceLoggerHandle
advapi32.dll.GetTraceEnableLevel
advapi32.dll.GetTraceEnableFlags
advapi32.dll.TraceEvent
mscoree.dll.IEE
mscoreei.dll.IEE
mscorwks.dll.IEE
mscoree.dll.GetStartupFlags
mscoreei.dll.GetStartupFlags
mscoree.dll.GetHostConfigurationFile
mscoreei.dll.GetHostConfigurationFile

mscoreei.dll.GetCORVersion
mscoree.dll.GetCORSystemDirectory
mscoreei.dll.GetCORSystemDirectory_RetAddr
mscoreei.dll.CreateConfigStream
ntdll.dll.RtlUnwind
kernel32.dll.IsWow64Process
advapi32.dll.AllocateAndInitializeSid
advapi32.dll.OpenProcessToken
advapi32.dll.GetTokenInformation

DELETED FILES

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.2756.17629234
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.2756.17629234
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2756.17629250
C:\Users\user\AppData\Roaming\Java\JavaUpdtr.exe:Zone.Identifier

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_CURRENT_USER\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\OnlyUseLatestCLR
Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\Standards\v2.0.50727
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStart
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStartAtJit

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\AppPatch
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\AppPatch\v4.0.30319.00000
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\AppPatch\v4.0.30319.00000\mscorwks.dll
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\e38a9f88f272ad1c712d369384f5fb9770b804ca.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\VersioningLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks
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\Security\Policy\Extensions\NamedPermissionSets
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets\Internet
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets\LocalIntranet
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\v2.0.50727\Security\Policy
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126\NIUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126\ILUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigString

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\EvalationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\LastModTime
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\GACChangeNotification\Default
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\mscorlib,2.0.0.0,,b77a5c561934e089,x86
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\2975157b\1f0e7108
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\policy.8.0.Microsoft.VisualBasic__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\1c22df2f\4f99a7c9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\1c22df2f\4f99a7c9\2e

EXECUTED COMMANDS

"C:\Users\user\AppData\Local\Temp\e38a9f88f272ad1c712d369384f5fb9770b804ca.exe"
C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding

READ FILES

C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Users\user\AppData\Local\Temp\e38a9f88f272ad1c712d369384f5fb9770b804ca.exe.config
C:\Users\user\AppData\Local\Temp\e38a9f88f272ad1c712d369384f5fb9770b804ca.exe
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_32\index126.dat
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\62a0b3e4b40ec0e8c5cfaa0c8848e64a\mscorlib.ni.dll
\Device\KsecDD
C:\Windows\System32\l_intl.nls
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\NativeImages_v2.0.50727_32\System\9e0a3b9b9f457233a335d7fba8f95419\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\08d608378aa405adc844f3cf36974b8c\Microsoft.VisualBasic.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\dbfe8642a8ed7b2b103ad28e0c96418a\System.Drawing.ni.dll
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Windows\Microsoft.NET\Framework\v2.0.50727\Culture.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorrc.dll
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\3afcd5168c7a6cb02eab99d7fd71e102\System.Windows.Forms.ni.dll
C:\Windows\System32\wbem\wbemdisp.tlb
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Windows\assembly\NativeImages_v2.0.50727_32\CustomMarshalers\bf7e7494e75e32979c7824a07570a8a9\CustomMarshalers.ni.dll
C:\Windows\assembly\GAC_32\CustomMarshalers\2.0.0.0__b03f5f7f11d50a3a\CustomMarshalers.dll
C:\Windows\SysWOW64\stdole2.tlb
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management\6f3b99ed0b791ff4d8aa52f2f0cd0bcf\System.Management.ni.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\wminet_utils.dll
C:\Windows\System32\tzres.dll
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Security\d9a485330ec2708456134e4a9712a4ab\System.Security.ni.dll

C:\Users\user\AppData\Roaming\Mozilla\SeaMonkey\profiles.ini
C:\Users\user\AppData\Roaming\Flock\Browser\profiles.ini
C:\Program Files (x86)\Mozilla Firefox\msvcr120.dll
C:\Program Files (x86)\Mozilla Firefox\msvcp120.dll
C:\Program Files (x86)\Mozilla Firefox\mozglue.dll
C:\Program Files (x86)\Mozilla Firefox\nss3.dll
C:\Windows\System32\winmm.dll
C:\Windows\System32\wsock32.dll
C:\Program Files (x86)\Mozilla Firefox\softokn3.dll
C:\Program Files (x86)\Mozilla Firefox\nssdbm3.dll
C:\Users\user\AppData\Roaming\Flock\Browser\secmod.db
C:\Program Files (x86)\Mozilla Firefox\freebl3.dll
C:\Users\user\AppData\Roaming\Flock\Browser\cert8.db
C:\Users\user\AppData\Roaming\Flock\Browser\cert7.db
C:\Users\user\AppData\Roaming\Flock\Browser\signons3.txt
C:\Users\user\AppData\Roaming\Thunderbird\profiles.ini
C:\Users\user\AppData\Roaming\FileZilla\recentservers.xml
C:\Users\user\AppData\Roaming\CoreFTP\sites.idx
C:\Windows\SysWOW64\wshom.ocx
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\bc09ad2d49d8535371845cd7532f9271\System.Configuration.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\461d3b6b3f43e6fbe6c897d5936e17e4\System.Xml.ni.dll
C:\Users\user\AppData\Roaming\ScreenShot\screen.jpeg
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
C:\Windows\Globalization\Sorting\sortdefault.nls
\??\WMIDataDevice
C:\Windows\Branding\Basebrd\basebrd.dll

C:

MUTEXES

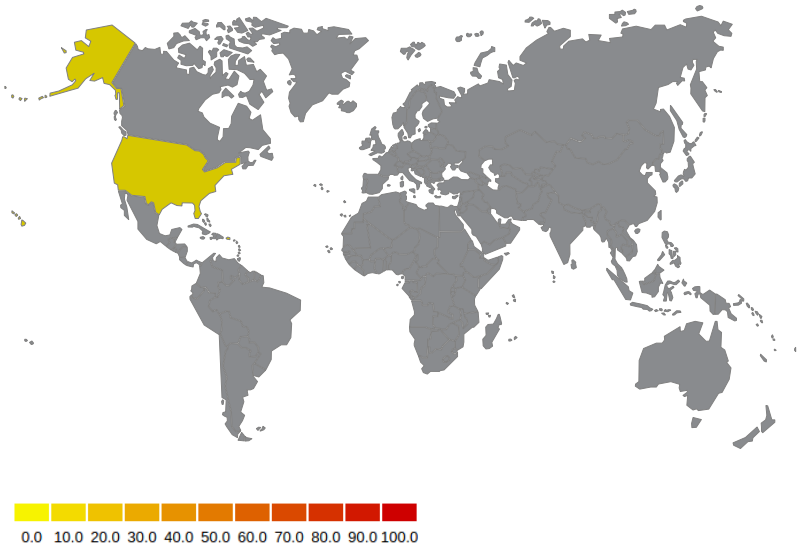
Global\CLR_CASOFF_MUTEX
Local_!MSFTHISTORY!_
Local\c:!users!user!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Local\c:!users!user!appdata!roaming!microsoft!windows!cookies!
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!
Global\.net clr networking

MODIFIED REGISTRY KEYS

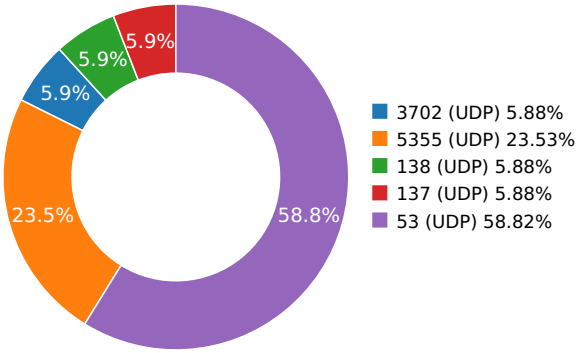
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Tregain
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\e38a9f88f272ad1c712d369384f5fb9770b804ca_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\e38a9f88f272ad1c712d369384f5fb9770b804ca_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\e38a9f88f272ad1c712d369384f5fb9770b804ca_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\e38a9f88f272ad1c712d369384f5fb9770b804ca_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\e38a9f88f272ad1c712d369384f5fb9770b804ca_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\e38a9f88f272ad1c712d369384f5fb9770b804ca_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\e38a9f88f272ad1c712d369384f5fb9770b804ca_RASAPI32\FileDirectory
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
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\ESS\//./root/CIMV2\SCM Event Provider

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 Communications, Inc.	Malware Process
	8.8.8.8	United States	15169	Level 3 Communications, Inc.	Malware Process

DNS QUERIES

Request	Type
checkip.dyndns.org	A
mail.cottonartprinters.com	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.04010891914	Sandbox	224.0.0.252	5355
3.04141592979	Sandbox	224.0.0.252	5355
3.05127906799	Sandbox	239.255.255.250	3702
3.07921290398	Sandbox	192.168.56.255	137
5.60280799866	Sandbox	224.0.0.252	5355
9.07898306847	Sandbox	192.168.56.255	138
64.3057889938	Sandbox	224.0.0.252	5355
67.1327850819	Sandbox	8.8.4.4	53
68.1254270077	Sandbox	8.8.8.8	53
85.479872942	Sandbox	8.8.8.8	53
86.4690508842	Sandbox	8.8.4.4	53
111.031970978	Sandbox	8.8.8.8	53
112.031847954	Sandbox	8.8.4.4	53
122.621435881	Sandbox	8.8.8.8	53
122.709560871	Sandbox	8.8.8.8	53
123.609823942	Sandbox	8.8.4.4	53
123.703356981	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Windows\History\History.IE5\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 645ccdde38bb039eb271a4f120e6be5f **SHA-1 :** 475a264964d84a2c6c335202262fa6c76275a515 **SHA-256 :** a9b45e98f41bfcc23bc82cf17b3381b9820a2be6c **SHA-512 :** 0f5aa71c7c0b1a574c4a6c306a24006ad175e7c8 **Size :** 49.152 Kilobytes.
C:\Users\User\AppData\Roaming\Java\JavaUpdtr.Exe	**Type :** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 461256eec678cf899ac154263c2d8c4d **SHA-1 :** e38a9f88f272ad1c712d369384f5fb9770b804ca **SHA-256 :** 89648f2fa7f77d968a87ab5fb61093f312f332adf5 **SHA-512 :** 771278634b5dab048f39ec25b58f19de105f9ad7 **Size :** 233.472 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** de20f795b0ea29cbcb8daf8951530db4 **SHA-1 :** 81d7e8a0197a0ea9eba76e4dc856d10aa5ec04d9 **SHA-256 :** f891c989c74d22028cc0dfcd564c186fe6857592c **SHA-512 :** 06ed0fdb0abfcdbc16a7f5adb92ed0c59ba788f08 **Size :** 180.224 Kilobytes.
C:\Users\User\AppData\Roaming\ScreenShot\Screen.Jpeg	**Type :** JPEG image data, JFIF standard 1.01 **MD5 :** 987aa523a0812dda1b56ba224d79e999 **SHA-1 :** a81eca93323abdbc341bcfb3da79d4189a457c1f **SHA-256 :** d7e4903c4a168120bcce9cf4dbda046c76549737 **SHA-512 :** 5f833bdfee6369627d5b1976b43d87e56fde21ec **Size :** 11.181 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 2ed7b584633888df7f0114fa4ac6dc69 **SHA-1 :** fa8067b3241b8d9258d9fc88f5bd80fca5433b10 **SHA-256 :** 69a0d29dc846c82d785231dbf94e4c4b731ad588 **SHA-512 :** 678165bd37def22a10615aded1384e97413fce1f **Size :** 32.768 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	Transfer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1:	e38a9f88f272ad1c712d369384f5fb9770b804ca
MD5:	461256eec678cf899ac154263c2d8c4d
First Seen Date:	2017-06-17 22:58:49.053217 (2 years ago)
Number Of Clients Seen:	2
Last Analysis Date:	2017-06-17 22:58:49.053217 (2 years ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
File Type Enum	6
Number Of Sections	3
Compilation Time Stamp	0x5945070A [Sat Jun 17 10:40:10 2017 UTC]
Translation	0x0000 0x04b0
LegalCopyright	Copyright (c) 2003-2007 Onno Broekmans
Assembly Version	11.12.13.15
InternalName	kosi.exe
FileVersion	17.8.12.18
CompanyName	Aestan Software
LegalTrademarks	Aestan Tray Menu
Comments	Aestan Tray Menu
ProductName	Tray Menu
ProductVersion	17.8.12.18
FileDescription	Aestan Software
OriginalFilename	kosi.exe
Entry Point	0x4372ae (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	233472
Sha256	89648f2fa7f77d968a87ab5fb61093f312f332adf5b9d4e4d18723ba7e4228e9
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x2000	0x352b4	0x36000	7.70372385007	7fec6e14f2c58dde69cbb3647da6404d
.rsrc	0x38000	0xc00	0x1000	2.15713204847	bf39731b09430334f92d80f3185669bb
.reloc	0x3a000	0xc	0x1000	0.0164084645156	84d66238820a6da1fa7e287b125d1c7f

PE Imports

- mscoree.dll
  - _CorExeMain

PE Resources

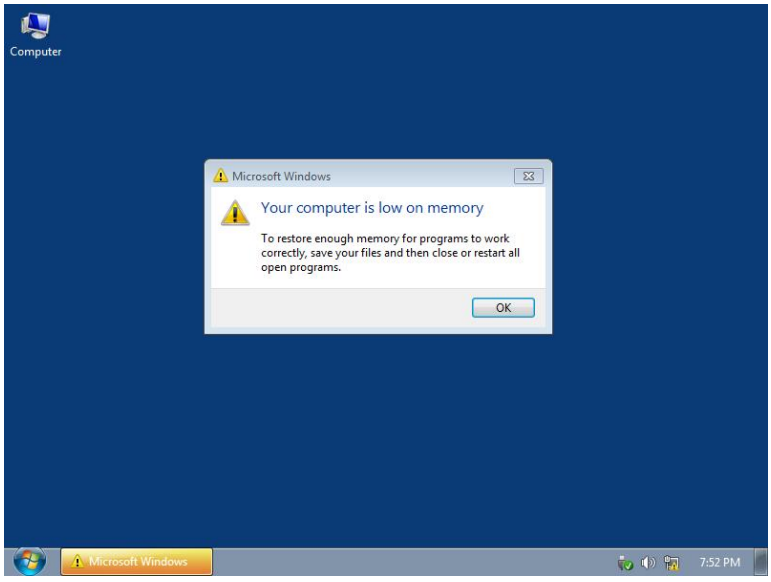
RT_ICON
RT_GROUP_ICON

RT_VERSION

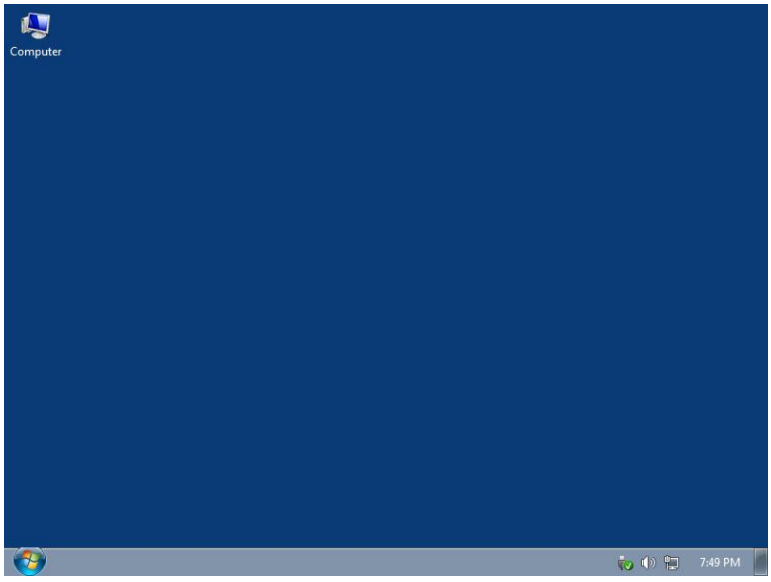
CERTIFICATE VALIDATION

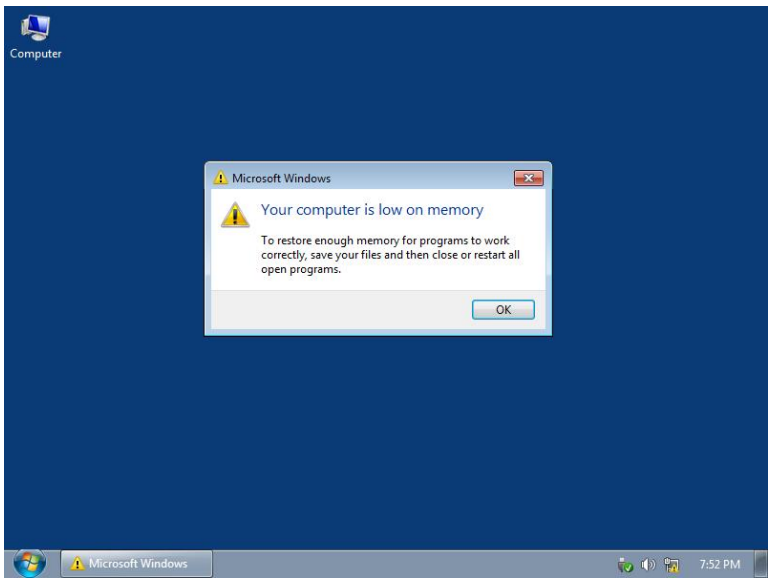
- Certificate Validation is not Applicable ?

SCREENSHOTS




Computer
7:50 PM


Computer
7:49 PM


Computer
Microsoft Windows
Your computer is low on memory
To restore enough memory for programs to work correctly, save your files and then close or restart all open programs.
OK
Microsoft Windows
7:52 PM