VALKYRIE COMODO

Summary

File Name: install_flash_player_13_plugin.exe

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

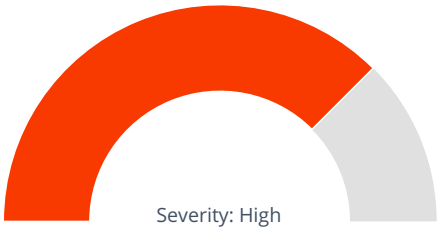
SHA1: 82b4f00f0ca92339ac824880a1c3340d3b94e235

MD5: b72aa215e37561ba3309b1b576b90177

MALWARE

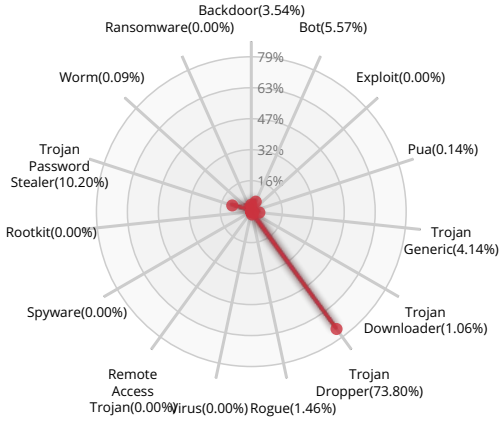
Valkyrie Final Verdict

DETECTION SECTION

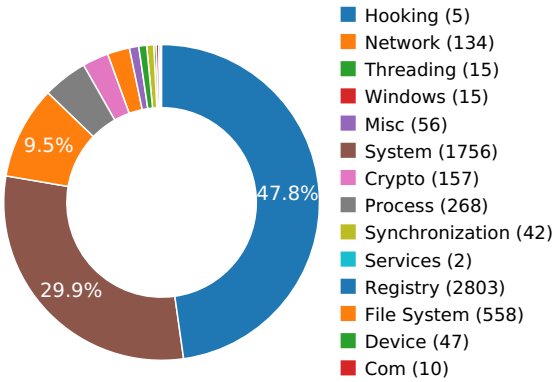


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image Show sources

NETWORKING

Starts servers listening on 127.0.0.1:0

CRYPTOGRAPHY

At least one IP Address, Domain, or File Name was found in a crypto call Show sources

PACKER

The binary likely contains encrypted or compressed data. Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

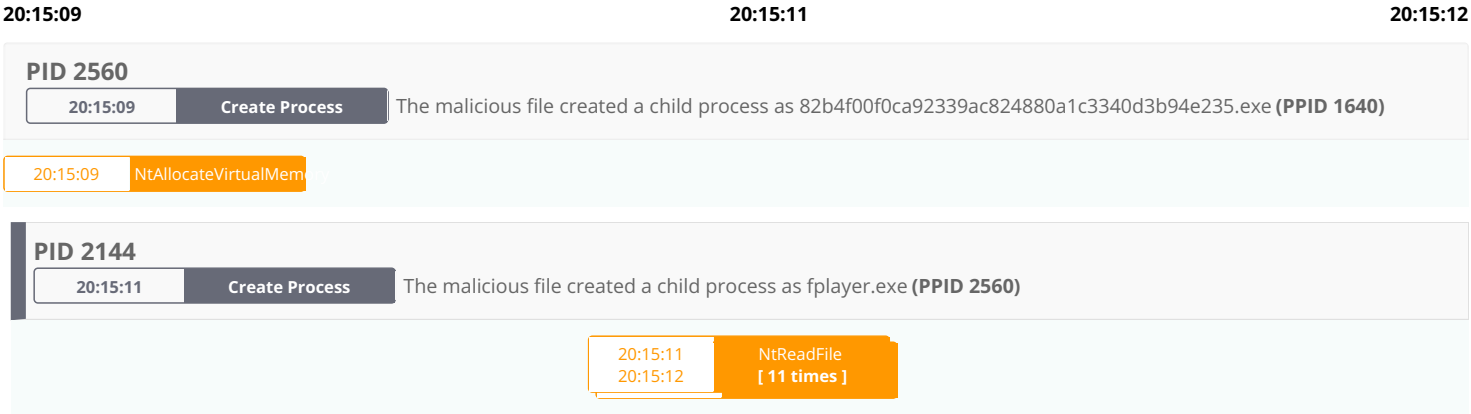
Creates RWX memory

DATA OBFUSCATION

Drops a binary and executes it Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\sysnative\MSCOREE.DLL.local
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework64*
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\clr.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
C:\Users\user\AppData\Local\Temp\82b4f00f0ca92339ac824880a1c3340d3b94e235.exe.config
C:\Users\user\AppData\Local\Temp\82b4f00f0ca92339ac824880a1c3340d3b94e235.exe
C:\Users\user\AppData\Local\Temp\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\sysnative\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\sysnative\wbem\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\sysnative\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\82b4f00f0ca92339ac824880a1c3340d3b94e235.exe.Local\
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\msvcr80.dll
C:\Windows
C:\Windows\winsxs
C:\Windows\Microsoft.NET\Framework64\v4.0.30319
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\fusion.localgac

C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_64\index142.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\9469491f37d9c35b596968b206615309\mscorlib.ni.dll
C:\Windows\assembly\GAC_64\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\Framework64\v2.0.50727\ole32.dll
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\82b4f00f0ca92339ac824880a1c3340d3b94e235.config
C:\Users\user\AppData\Local\Temp\82b4f00f0ca92339ac824880a1c3340d3b94e235.INI
C:\Windows\sysnative\l_intl.nls
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\GAC\PublisherPolicy.tme
C:\Windows\assembly\NativeImages_v2.0.50727_64\System\adff7dd9fe8e541775c46b6363401b22\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\5910828a337dbe848dc90c7ae0a7dee2\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Windows.Forms\6c352ff9e3603b0e69d969ff7e7632f5\System.Windows.Forms.ni.dll
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.INI
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.INI
C:\Windows\assembly\GAC_MSIL\System.Drawing\2.0.0.0__b03f5f7f11d50a3a\System.Drawing.INI
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\uxtheme.dll
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll
C:\Windows\Globalization\en-us.nlp
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Gdiplus.dll
C:\Windows\winsxs\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437a
C:\Windows\winsxs\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437a\GdiPlus.dll
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT

C:\Windows\Fonts\ahronbd.ttf
C:\Windows\Fonts\tahoma.ttf
C:\Windows\Fonts\msjh.ttf
C:\Windows\Fonts\msyh.ttf
C:\Windows\Fonts\malgun.ttf
C:\Windows\Fonts\micross.ttf
C:\Windows\Fonts\segoeui.ttf
C:\Windows\Fonts\staticcache.dat
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\CLRLoadLogDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\OnlyUseLatestCLR
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\GCStressStart
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\GCStressStartAtJit
HKEY_LOCAL_MACHINE\SOFTWARE\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\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142\NIUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142\ILUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\EvalationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\mscorlib,2.0.0.0,,b77a5c561934e089,AMD64
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\CseOn
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\TailCallOpt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\PInvokeInline
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\PInvokeCalliOpt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\NewGCCalc
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\TURNOFFDEBUGINFO
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\DisableHotCold
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_64\NI\61e7e666\c991064\83\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\61e7e666\c991064\83\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\61e7e666\c991064\83\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\61e7e666\c991064\83\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\61e7e666\c991064\83\EvalationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\61e7e666\c991064\83\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\61e7e666\c991064\83\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\61e7e666\c991064\83\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\61e7e666\c991064\83\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\475dce40\2d382ce6\8d\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\475dce40\2d382ce6\8d\Status

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\475dce40\2d382ce6\8d\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\475dce40\2d382ce6\8d\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\475dce40\2d382ce6\8d\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\19ab8d57\1bd7b0d8\8f\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\19ab8d57\1bd7b0d8\8f\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\19ab8d57\1bd7b0d8\8f\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\19ab8d57\1bd7b0d8\8f\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\19ab8d57\1bd7b0d8\8f\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\2dd6ac50\163e1f5e\8a\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\2dd6ac50\163e1f5e\8a\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\2dd6ac50\163e1f5e\8a\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\2dd6ac50\163e1f5e\8a\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\2dd6ac50\163e1f5e\8a\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\424bd4d8\1c83327b\8e\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\424bd4d8\1c83327b\8e\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\424bd4d8\1c83327b\8e\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\424bd4d8\1c83327b\8e\SIG

MODIFIED FILES

C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
C:\Users\user\AppData\Local\fplayer.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

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
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.RtlVirtualUnwind
kernel32.dll.IsWow64Process
advapi32.dll.AllocateAndInitializeSid
advapi32.dll.OpenProcessToken
advapi32.dll.GetTokenInformation
advapi32.dll.InitializeAcl

DELETED FILES

C:\Users\user\AppData\Local\fplayer.exe

C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch.2560.17662343

C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.2560.17662343

C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.2560.17662406

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\LowRegistry\AddToFavoritesInitialSelection

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\LowRegistry\AddToFeedsInitialSelection

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\v4.0

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\InstallRoot

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\CLRLoadLogDir

HKEY_CURRENT_USER\Software\Microsoft\.NETFramework

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\OnlyUseLatestCLR

Policy\Standards

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\Standards

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\standards\v2.0.50727

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\GCStressStart

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\GCStressStartAtJit

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\DisableConfigCache

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\AppPatch

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\AppPatch\v4.0.30319.00000

HKEY_LOCAL_MACHINE\SOFTWARE\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\82b4f00f0ca92339ac824880a1c3340d3b94e235.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\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\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets\Internet
HKEY_LOCAL_MACHINE\SOFTWARE\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_64
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142\NIUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142\ILUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\EvalationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\Status

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\IL\7950e2c5\19b8f67f\82\LastModTime
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\GACChangeNotification\Default
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\mscorlib,2.0.0.0,,b77a5c561934e089,AMD64
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\38980725\62942ee5
HKEY_LOCAL_MACHINE\Software\Microsoft\StrongName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\CseOn
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\TailCallOpt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\PInvokeInline
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\PInvokeCalliOpt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\NewGCCalc
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\TURNOFFDEBUGINFO
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\DisableHotCold
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\internal\jit\Perf

READ FILES

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Users\user\AppData\Local\Temp\82b4f00f0ca92339ac824880a1c3340d3b94e235.exe.config
C:\Users\user\AppData\Local\Temp\82b4f00f0ca92339ac824880a1c3340d3b94e235.exe
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\msvcr80.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_64\index142.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\9469491f37d9c35b596968b206615309\mscorlib.ni.dll
\Device\KsecDD
C:\Windows\sysnative\l_intl.nls
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorjit.dll
C:\Windows\assembly\pubpol20.dat

C:\Windows\assembly\NativeImages_v2.0.50727_64\System\adff7dd9fe8e541775c46b6363401b22\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\5910828a337dbe848dc90c7ae0a7dee2\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Windows.Forms\6c352ff9e3603b0e69d969ff7e7632f5\System.Windows.Forms.ni.dll
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll
C:\Windows\winsxs\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437a\GdiPlus.dll
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
C:\Windows\Fonts\tahoma.ttf
C:\Windows\Fonts\msjh.ttf
C:\Windows\Fonts\msyh.ttf
C:\Windows\Fonts\malgun.ttf
C:\Windows\Fonts\micross.ttf
C:\Windows\Fonts\segoeui.ttf
C:\Windows\Fonts\staticcache.dat
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Culture.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorrc.dll
C:\Windows\System32\tzres.dll
C:\Users\user\AppData\Local\fplayer.exe
C:\Windows\System32\p2pcollab.dll
C:\Windows\System32\dnsapi.dll
C:\Windows\System32\en-US\dnsapi.dll.mui
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\A092A81885DDD5AAD1EC1A803D7183779D81B6F9
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\BAED8A8C5A147CFA78E686BB4A8E5829C2F934F5
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\C8A51E044BF5AF39158BB24E414E8FDCD2891C3A
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\FB45378AB288E369B22C860D123A809F530D5CC1
C:\Windows\System32\shell32.dll
C:\
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004a.db
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\Desktop\desktop.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

MUTEXES

Global\CLR_CASOFF_MUTEX
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Adobe Acrobat Installer-EXCLUSIVE
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!

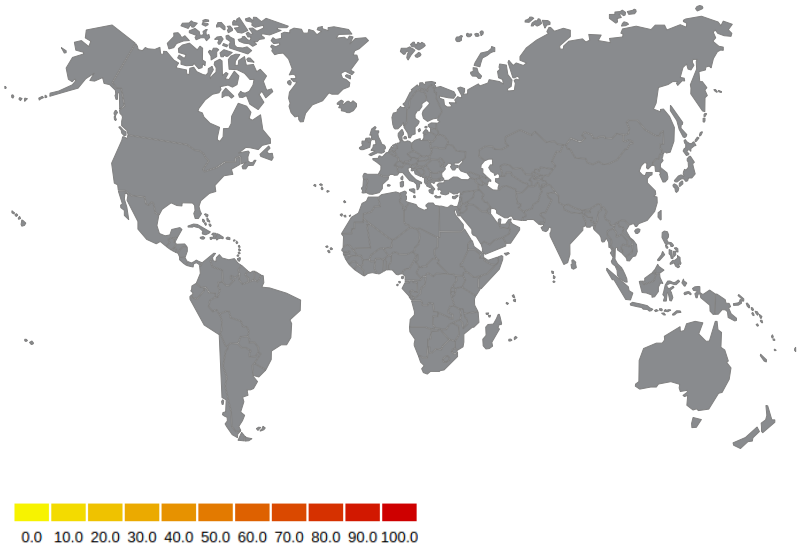
MODIFIED REGISTRY KEYS

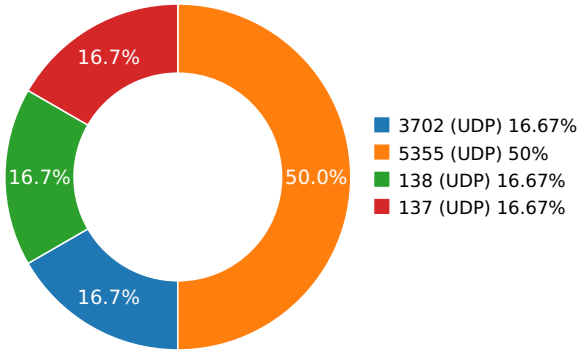
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042

HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103

Network Behavior

CONTACTED IPS	NETWORK PORT DISTRIBUTION





Name	IP	Country	ASN	ASN Name	Trigger Process Type

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.1542069912	Sandbox	224.0.0.252	5355
3.18512821198	Sandbox	224.0.0.252	5355
3.1914191246	Sandbox	239.255.255.250	3702
3.20683002472	Sandbox	192.168.56.255	137
5.73866605759	Sandbox	224.0.0.252	5355
6.21871519089	Sandbox	192.168.56.255	138

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\Local\Fplayer.Exe	**Type :** MS-DOS executable, MZ for MS-DOS **MD5 :** 0cca673d5ddb45871d05f6a733059e56 **SHA-1 :** 77f250c949e5f7d3e7ba33968c74428740fa1031 **SHA-256 :** 6c121282c56f9c651fa0c56c9b495b55cd56f7a9f **SHA-512 :** 7adc51286afd0cd3c2e91be2c50dfeae010846fcc **Size :** 1055.936 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\Local\GDIPFONTCACHEV1.DAT	**Type :** data **MD5 :** 696bad2ef23da7f0ccaaa7f76ab9fdf0 **SHA-1 :** 0efe907b47e8331cf56a95c0c06d324257ece202 **SHA-256 :** bd27979561fac15e4043fc980ad62f24f00738cba **SHA-512 :** fb1a4afdbf5f9e3d7e55eb806f660057927d6c357 **Size :** 84.528 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:	install_flash_player_13_plugin.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1:	82b4f00f0ca92339ac824880a1c3340d3b94e235
MD5:	b72aa215e37561ba3309b1b576b90177
First Seen Date:	2017-06-17 18:47:23.971421 (2 years ago)
Number Of Clients Seen:	2
Last Analysis Date:	2017-06-17 18:47:23.971421 (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	0x593E9ED7 [Mon Jun 12 14:01:59 2017 UTC]
Translation	0x0000 0x04b0
LegalCopyright	Copyright \xa9 2017
Assembly Version	1.0.0.0
InternalName	install_flash_player_13_plugin.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	install_flash_player_13_plugin
ProductVersion	1.0.0.0
FileDescription	install_flash_player_13_plugin
OriginalFilename	install_flash_player_13_plugin.exe
Entry Point	0x50521a (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	1093632
Sha256	e5682c3c4df451b0cdee9bb2f7bf9a809cf5923d14a87340c49679fff9715ba9
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x2000	0x103220	0x103400	7.91943752205	bdb53f7338ef54b049e3d6d0e1a3428b
.rsrc	0x106000	0x7778	0x7800	4.11542647274	32126d641edb4749b2248de219b1aa6d
.reloc	0x10e000	0xc	0x200	0.101910425663	2768cf7329a7a059f24fdefaca0a6b75

PE Imports

- mscoree.dll
  - _CorExeMain

PE Resources

RT_ICON
RT_GROUP_ICON

RT_VERSION
RT_MANIFEST

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS