Summary

File Name: ud8qQSCc7kEdZKzblmZWqRhCfNo79m7T

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

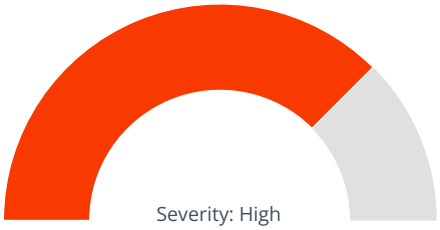
SHA1: e541b15427e08d8c0ea7bb03080e6341dba1672f

MD5: 8adee9dce45b8d418ce98bb23d8c1c62

MALWARE

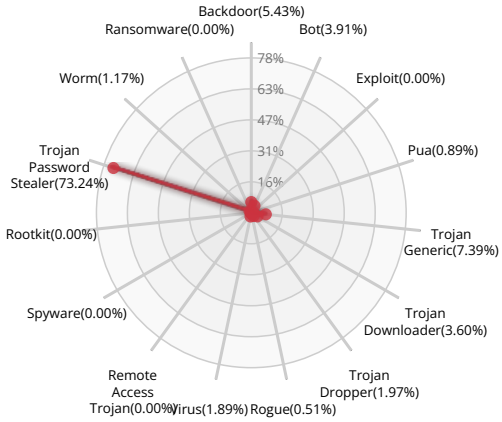
Xcitium Verdict Cloud Final Verdict

DETECTION SECTION

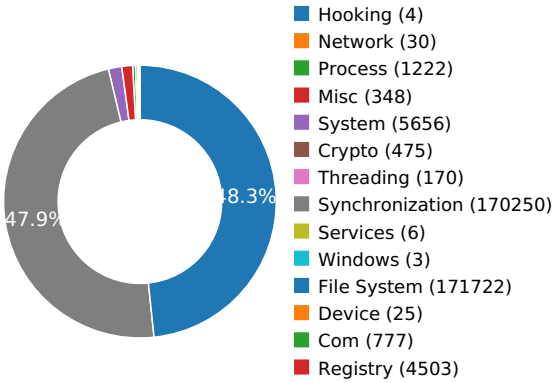


Verdict: Malware

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

Steals private information from local Internet browsers Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task. Show sources

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

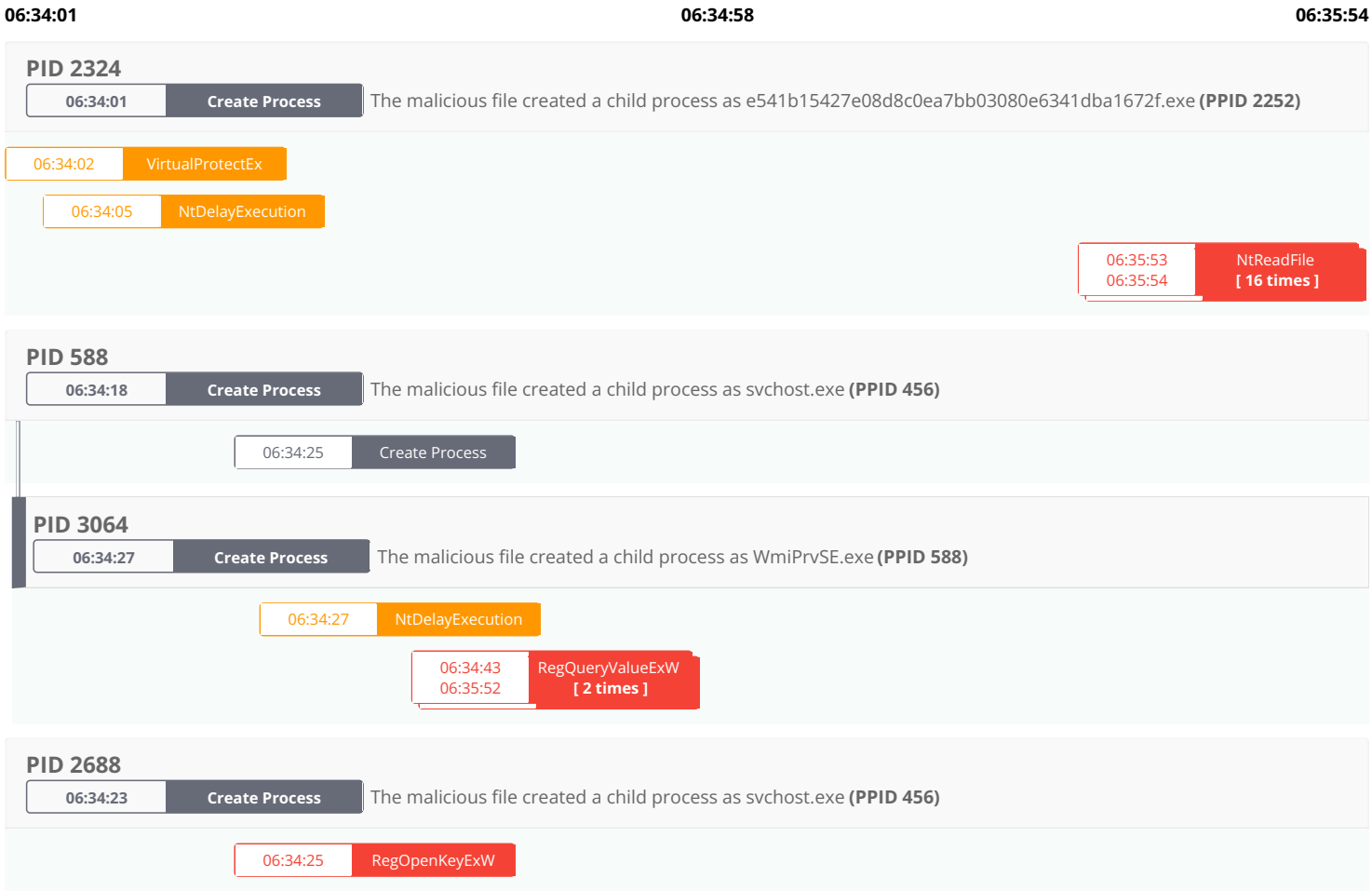
HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

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\e541b15427e08d8c0ea7bb03080e6341dba1672f.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\Wow6432Node\Microsoft\Windows NT\CurrentVersion\ProductName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\CSDVersion
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\92ABECA0
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\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

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\e541b15427e08d8c0ea7bb03080e6341dba1672f.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.Joker__461d39c4a423da0b
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.1.9.Joker__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\e541b15427e08d8c0ea7bb03080e6341dba1672f.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

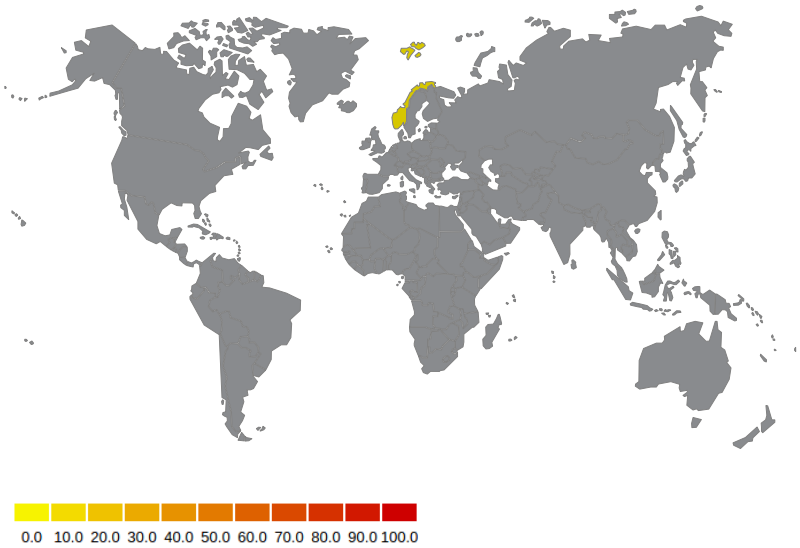
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite
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

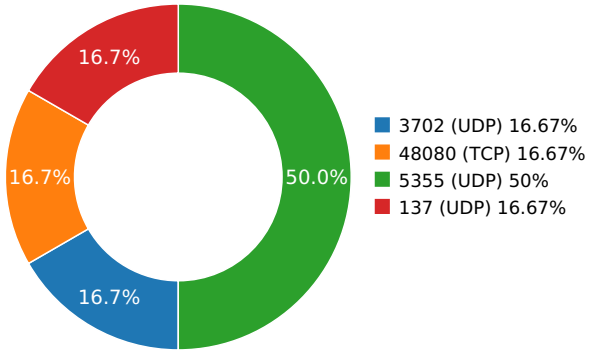
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Transports\Decoupled\Server
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\CreationTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\MarshaledProxy
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
	146.59.161.7	Norway	16276	Failover Ips	Malware Process

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
9.40358519554	Sandbox	146.59.161.7	48080

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.00844407082	Sandbox	224.0.0.252	5355
3.03191709518	Sandbox	224.0.0.252	5355
3.03848099709	Sandbox	239.255.255.250	3702
3.07990598679	Sandbox	192.168.56.255	137
5.62671399117	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:	ud8qQSCc7kEdZKzblmZWqRhCfNo79m7T
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	e541b15427e08d8c0ea7bb03080e6341dba1672f
MD5:	8adee9dce45b8d418ce98bb23d8c1c62
First Seen Date:	2023-07-03 21:50:35.555538 (a day ago)
Number Of Clients Seen:	3
Last Analysis Date:	2023-07-03 21:50:35.555538 (a day ago)
Human Expert Analysis Date:	2023-07-04 10:34:15.671363 (about 13 hours 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	[]
Number Of Sections	4
Trid	[[42.2, u'Win32 Executable MS Visual C++ (generic)'], [37.3, u'Win64 Executable (generic)'], [8.8, u'Win32 Dynamic Link Library (generic)'], [6.0, u'Win32 Executable (generic)'], [2.7, u'Generic Win/DOS Executable']]
Compilation Time Stamp	0x62792EE4 [Mon May 9 15:10:28 2022 UTC]
InternalName	HondaForza.exe
LegalTrademarks2	unobservable
FileVersion	88.53.80.23
CompanyName	History
FileDescriptions	Blast
ProductName	FreewayTrip
ProductVersion	57.71.45.5
LegalCopyrights	Challengers mazambik inc.
Translation	0x4250 0x03ff
Entry Point	0x4058cc (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	358400
Ssdeep	6144:VBkESC272XNJSjjkE1aaQYrv6BTokELZGi7HM8SO:cRC272Xy//AJ61LpMbO
Sha256	98f91b9e77276b58e267d61783f27c9a5af536427bbdc37f1e1bc98260696bdf
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'EXE:FileDescriptions': u'Blast', u'EXE:LegalCopyrights': u'Challengers mazambik inc.', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/e/5/4/1/e541b15427e08d8c0ea7bb03080e6341dba1672f', u'EXE:ProductName': u'FreewayTrip', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2023:07:03 21:49:32+00:00', u'EXE:InitializedDataSize': 24388096, u'File:FileModifyDate': u'2023:07:03 21:49:31+00:00', u'EXE:LinkerVersion': 10.0, u'EXE:FileVersionNumber': u'100.0.0.0', u'EXE:FileVersion': u'88.53.80.23', u'File:FileSize': u'350 kB', u'EXE:CharacterSet': u'Unknown (85B1)', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Windows NT 32-bit', u'EXE:ProductVersion': u'57.71.45.5', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'History', u'File:FileName': u'e541b15427e08d8c0ea7bb03080e6341dba1672f', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 5.1, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2022:05:09 15:10:28+00:00', u'EXE:LegalTrademarks2': u'unobservable', u'EXE:FileFlagsMask': u'0x003f', u'EXE:InternalName': u'HondaForza.exe', u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/e/5/4/1', u'EXE:EntryPoint': u'0x58cc', u'EXE:SubsystemVersion': 5.1, u'EXE:CodeSize': 119808, u'File:FileInodeChangeDate': u'2023:07:03 21:49:31+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'Unknown (0291)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'2.0.0.0'}]
Mime Type	application/x-dosexec
Imphash	144f161f98acce6fa2a99dd080adf6b9

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x1d21a	0x1d400	4.86962561467	0f029c4eb2caed5310c40b731ca80da9
.data	0x1f000	0x1728d8c	0x29800	7.96439781296	46528a011f7a81fce096b5332fddaa8e
.yalibe	0x1748000	0x244	0x400	0.0	0f343b0931126a20f133d67c2b018a3b
.rsrc	0x1749000	0x102a0	0x10400	3.66325281327	f8cdce1d5450b57b07017dc1353d2f34

PE Imports

- KERNEL32.dll
  - CreateMutexW
  - WriteConsoleInputW
  - AllocConsole
  - lstrcpynA
  - HeapAlloc
  - InterlockedIncrement
  - InterlockedDecrement
  - GetNamedPipeHandleStateA
  - GetUserDefaultLCID
  - GetModuleHandleW
  - GetTickCount
  - GetCurrentThread
  - GetConsoleAliasesLengthA
  - GetWindowsDirectoryA
  - GetCompressedFileSizeW
  - GetConsoleAliasExesW
  - WaitNamedPipeW
  - GetCommandLineA
  - GetPriorityClass
  - GetVolumePathNameW
  - GetPrivateProfileIntA
  - SetFileShortNameW
  - _hread
  - GetCalendarInfoW
  - CreateEventA
  - GetConsoleAliasExesLengthW
  - GetFileAttributesA
  - CreateSemaphoreA
  - WriteConsoleW
  - IsDBCSLeadByte
  - QueryInformationJobObject
  - CompareStringW
  - GetACP
  - lstrlenW
  - FindNextVolumeMountPointW
  - SetThreadPriority
  - GetTempFileNameW
  - EnumSystemLocalesA
  - DeleteFiber
  - GetLastError
  - GetProcAddress
  - HeapSize
  - BeginUpdateResourceW
  - RemoveDirectoryA
  - SetComputerNameA
  - EnterCriticalSection
  - SearchPathA
  - SetFileAttributesA
  - LoadLibraryA
  - OpenWaitableTimerW
  - LocalAlloc
  - MoveFileA
  - GetNumberFormatW
  - AddAtomW
  - OpenJobObjectW
  - FindAtomA
  - GetPrivateProfileSectionNamesA
  - GetModuleHandleA
  - OpenFileMappingW
  - FreeEnvironmentStringsW

    - FindNextFileW
    - GetStringTypeW
    - GetCurrentDirectoryA
    - EnumDateFormatsW
    - GetShortPathNameW
    - SetCalendarInfoA
    - GetVersionExA
    - GetFileInformationByHandle
    - DebugBreak
    - ReadConsoleOutputCharacterW
    - lstrcpyW
    - DeleteFileA
    - LocalFileTimeToFileTime
    - CreateMailslotW
    - GetVolumeNameForVolumeMountPointA
    - Sleep
    - InitializeCriticalSection
    - DeleteCriticalSection
    - LeaveCriticalSection
    - EncodePointer
    - DecodePointer
    - WideCharToMultiByte
    - HeapSetInformation
    - GetStartupInfoW
    - HeapFree
    - RtlUnwind
    - GetCPInfo
    - GetOEMCP
    - IsValidCodePage
    - TlsAlloc
    - TlsGetValue
    - TlsSetValue
    - TlsFree
    - SetLastError
    - GetCurrentThreadId
    - UnhandledExceptionFilter
    - SetUnhandledExceptionFilter
    - IsDebuggerPresent
    - TerminateProcess
    - GetCurrentProcess
    - SetFilePointer
    - CloseHandle
    - RaiseException
    - ExitProcess
    - WriteFile
    - GetStdHandle
    - GetModuleFileNameW
    - GetModuleFileNameA
    - GetEnvironmentStringsW
    - SetHandleCount
    - InitializeCriticalSectionAndSpinCount
    - GetFileType
    - HeapCreate
    - QueryPerformanceCounter
    - GetCurrentProcessId
    - GetSystemTimeAsFileTime
    - MultiByteToWideChar
    - IsProcessorFeaturePresent
    - LCMapStringW
    - SetStdHandle
    - GetConsoleCP
    - GetConsoleMode
    - FlushFileBuffers
    - LoadLibraryW
    - HeapReAlloc
    - ReadFile
    - CreateFileW
- ADVAPI32.dll
    - ReadEventLogA

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 24475840, u'sha256': u'9290ec1d55e739cae08232a2be51bfb9b40ca69ffd44e796d493b1e1d2cc2c2c', u'type': u'data', u'size': 304}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 24476168, u'sha256':

u'755c3646883985ad1d833271ae1e161293ac394342f70366fceea5cbc99163c4', u'type': u'dBase III DBT, version number 0, next free block index 40, 1st item "\\251\\317"', u'size': 2216}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24417936, u'sha256': u'473b3dc0103a23a9d5abcb6f19ef1149207891771df687705e4b5dc71f2182d6', u'type': u'data', u'size': 2216}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24420152, u'sha256': u'8d016fb9c92edcf1850f2f59859e29c53694fe4c95b6e8d9a2ecc75a452d56a0', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24424456, u'sha256': u'827d728d1c820464b12a9efd1db6a2b5e0c19bf5ae4f5648d49d47d5cae8afe0', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24428208, u'sha256': u'838fd9dbe2cc292d66985fe619a3c3b1b23616f35816aa6c73b39e1da4c75bc0', u'type': u'dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 8421249, next used block 8486785', u'size': 2216}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24430424, u'sha256': u'b3f2dadfbc25c0c7b0c9bc9e4a9560a6a7fa8e15ff6dca1a1f55d518626bcd75', u'type': u'data', u'size': 1736}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24432160, u'sha256': u'a7db661cf2baebd26701a8240230b7eef076b1c21276c594d9ec948bba70add7', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24433544, u'sha256': u'8d350f08329202b4cec021f5d6f0d50b6e37d3446609aae8692cd300f61f7869', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24443184, u'sha256': u'eb4a6da063e7784aea81129764c970b722fea271fa0dab93214c5cb4898b994a', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24447448, u'sha256': u'9fbedaf874b439e55201d4aa035fc21f92563d84c84eb54416de6131ebbbec1b', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24449888, u'sha256': u'9755fb3d3b909214b06f05f6c77588002cc757c7d84ef41ff36cf147053fd6b2', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24451136, u'sha256': u'f513b135c532198e665434e76e250c99144ab95dea3aa502928258ef7e89f14e', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24454888, u'sha256': u'5a9c99cfe749d148127358279e78f31ce7995f2d0effbc872757b8d734885fcc', u'type': u'data', u'size': 1736}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24456624, u'sha256': u'fc7bc3ef7fae01961560c42cb43f103df4704cd68c9a119d97593783b140a3db', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24458008, u'sha256': u'159675d9b23d89384868e9c9ce495eeec3417c37fb295fa0b968883eb9ba4ae3', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24467648, u'sha256': u'7f0bb3d548c32280b644f1d0c51e008d2bcc1b108b906e19a135359921015636', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24471912, u'sha256': u'2742f2772961300e72146e84c6710a21b4189c1cd19b55d7c2229881ec0d8029', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 2440}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ICON', u'offset': 24474352, u'sha256': u'65421a2ca72911d0a57fba2046b6f90db6cf7388e5fac91829e5a3c439570081', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_TAMIL', u'name': u'RT_STRING', u'offset': 24479128, u'sha256': u'263830501bd669e83adda456cf7db69f7542fc6e9be09db1d435db60474b294a', u'type': u'data', u'size': 780}

{u'lang': u'LANG_TAMIL', u'name': u'RT_STRING', u'offset': 24479912, u'sha256': u'eda3585e1c96a3d5c96e53e2b51e101e7c3e38817a9b5658d798a16c34b05eb9', u'type': u'data', u'size': 892}

{u'lang': u'LANG_TAMIL', u'name': u'RT_STRING', u'offset': 24480808, u'sha256': u'7a4812c8d8f749a728b9742263b3ffa6a986204a3ee03b5aabf28a55c3e88fcf', u'type': u'data', u'size': 780}

{u'lang': u'LANG_TAMIL', u'name': u'RT_STRING', u'offset': 24481592, u'sha256': u'bd196690e3b7ca69d418e1b68d8a8686609a50837cb6a8edac377c5c574bbe7f', u'type': u'data', u'size': 868}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ACCELERATOR', u'offset': 24475720, u'sha256': u'9b2d7d995e9dad1565597040980e1f68a7ddc8d6d6e6e4325331e0d477b44975', u'type': u'data', u'size': 120}

{u'lang': u'LANG_TAMIL', u'name': u'RT_ACCELERATOR', u'offset': 24475584, u'sha256': u'e94ddc2be1ecf7ad6811c0cd18c161169c4249c7fcf361eb94d4fb9becf44236', u'type': u'data', u'size': 136}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 24476144, u'sha256': u'460268b31726095b94bc0903e72b1853f08dc863ff255ea143173a9047106e16', u'type': u'MS Windows icon resource - 1 icon, 32x32, 2 colors', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 24478384, u'sha256': u'217d450a16a2372b00cba65fee0521ed845f5ced6dea83c12e37275f8bbbcc42', u'type': u'MS Windows icon resource - 1 icon, 32x32', u'size': 20}

{u'lang': u'LANG_TAMIL', u'name': u'RT_GROUP_ICON', u'offset': 24424416, u'sha256': u'365743600699d40fef274a86084ef5ec4abaf99a83a1adc852eff39efef7d24c', u'type': u'MS Windows icon resource - 2 icons, 32x32', u'size': 34}

{u'lang': u'LANG_TAMIL', u'name': u'RT_GROUP_ICON', u'offset': 24451016, u'sha256': u'69ec7901164492b9daeb674122ffd9ce6521afa84546e6bde2e9d97d69bb6e18', u'type': u'MS Windows icon resource - 8 icons, 48x48', u'size': 118}

{u'lang': u'LANG_TAMIL', u'name': u'RT_GROUP_ICON', u'offset': 24475480, u'sha256': u'95c3d8d9f5922917620fcfddf9c590d501fb9b4cdf881bd6ea5198cb729071b9', 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': 24478408, u'sha256': u'5bbbe58b1aff027d7efa45d6aabc087db65bcdfc528776c0e7479ed868cdeca9', u'type': u'data', u'size': 716}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS