Summary

File Name: bdbdc0e68f0175414075ae9841781c51ce3784d7

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

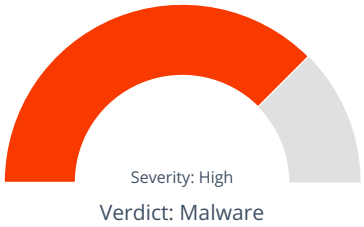
SHA1: bdbdc0e68f0175414075ae9841781c51ce3784d7

MD5: a494133a749128886cf99016e767f5dc

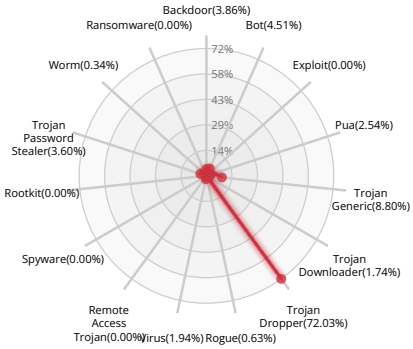
MALWARE

Xcitium Verdict Cloud Final Verdict

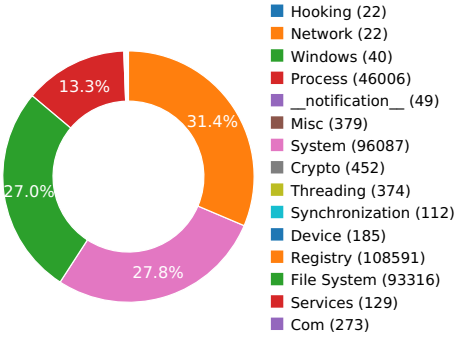
DETECTION SECTION



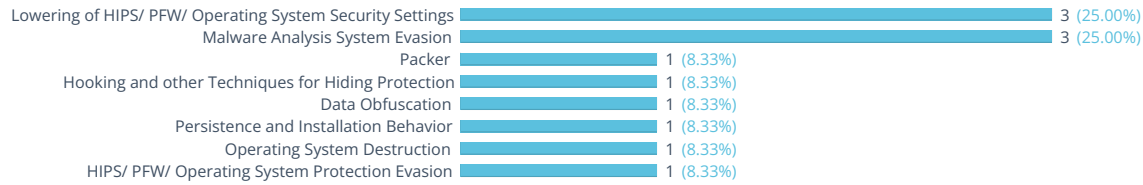
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



Activity Details

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

- Attempts to disable Windows Defender — Show sources
- Attempts to disable Windows Auto Updates — Show sources
- Attempts to block SafeBoot use by removing registry keys — Show sources

PACKER

- The binary likely contains encrypted or compressed data. — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

- Creates RWX memory — Show sources

DATA OBFUSCATION

- Drops a binary and executes it — Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

- Installs itself for autorun at Windows startup — Show sources

OPERATING SYSTEM DESTRUCTION

- At least one process apparently crashed during execution — Show sources

MALWARE ANALYSIS SYSTEM EVASION

- A process attempted to delay the analysis task. — Show sources
- Attempts to repeatedly call a single API many times in order to delay analysis time — Show sources
- Spoofs its process name and/or associated pathname to appear as a legitimate process — Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

- Attempts to stop active services — Show sources

Behavior Graph

12:00:44 Create Process
12:01:01 Create Process
12:01:31 Create Process
12:01:45 Create Process
12:02:14 GetSystemTimeAsFileTi
12:07:12 [26 times]
12:07:09 Create Process

PID 2844
11:59:18 Create Process The malicious file created a child process as TrustedInstaller.exe **(PPID 460)**

PID 2668
12:00:54 Create Process The malicious file created a child process as mscorsvw.exe **(PPID 460)**

PID 2820
12:00:59 Create Process The malicious file created a child process as mscorsvw.exe **(PPID 460)**

PID 1288
12:01:13 Create Process The malicious file created a child process as sppsvc.exe **(PPID 460)**

12:02:39 RegOpenKeyExW

PID 3044
12:01:33 Create Process The malicious file created a child process as svchost.exe **(PPID 460)**

12:01:33 LdrLoadDll
12:01:33 Create Process

PID 2100
12:01:33 Create Process The malicious file created a child process as WerFault.exe **(PPID 3044)**

PID 2704
12:01:44 Create Process The malicious file created a child process as taskhost.exe **(PPID 460)**

PID 1228
12:07:49 Create Process The malicious file created a child process as sc.exe **(PPID 460)**

PID 568
12:01:00 Create Process The malicious file created a child process as svchost.exe **(PPID 460)**

12:01:40 Create Process

PID 2340
12:01:28 Create Process The malicious file created a child process as WmiPrvSE.exe **(PPID 568)**

12:01:29 NtDelayExecution

PID 864
12:01:02 Create Process The malicious file created a child process as svchost.exe **(PPID 460)**

12:03:30 Create Process

PID 1944
12:03:48 Create Process The malicious file created a child process as WMIADAP.exe **(PPID 864)**

12:04:44 NtDelayExecution

PID 764
12:01:43 Create Process The malicious file created a child process as svchost.exe **(PPID 460)**

Behavior Summary

ACCESSED FILES

C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\IXP000.TMP
C:\Users\user\AppData\Local\Temp\IXP000.TMP\TMP4351$.TMP
C:\Users\user\AppData\Local\Temp\IXP000.TMP\
C:\
C:\Users\user\AppData\Local\Temp
C:\Windows
C:\Users\user\AppData\Local\Temp\IXP000.TMP\z8784040.exe
C:\Users\user\AppData\Local\Temp\IXP000.TMP\t1498787.exe
C:\Users\user\AppData\Local\Temp\IXP001.TMP
C:\Users\user\AppData\Local\Temp\IXP001.TMP\TMP4351$.TMP
C:\Users\user\AppData\Local\Temp\IXP001.TMP\
C:\Users\user\AppData\Local\Temp\IXP001.TMP\z7869856.exe
C:\Users\user\AppData\Local\Temp\IXP001.TMP\s6358817.exe
C:\Users\user\AppData\Local\Temp\IXP001.TMP*
C:\Users\user\AppData\Local\Temp\IXP002.TMP
C:\Users\user\AppData\Local\Temp\IXP002.TMP\TMP4351$.TMP
C:\Users\user\AppData\Local\Temp\IXP002.TMP\
C:\Users\user\AppData\Local\Temp\IXP002.TMP\p2889321.exe
C:\Users\user\AppData\Local\Temp\IXP002.TMP\r4984541.exe
C:\Users\user\AppData\Local\Temp\IXP002.TMP*
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:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe.config
C:\Windows\Microsoft.NET\Framework\v4.0.30319\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:\Users\user\AppData\Local\Temp\IXP002.TMP\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:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config
C:\Windows\Microsoft.NET\Framework\v4.0.30319\fusion.localgac
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\AppLaunch.exe
C:\Windows\Microsoft.NET
C:\Windows\Microsoft.NET\Framework
C:\Windows\Microsoft.NET\Framework\v4.0.30319
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ole32.dll
\Device\KsecDD
C:\Windows\assembly\NativeImages_v4.0.30319_32\Healer*
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.INI
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\GAC\PublisherPolicy.tme
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

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\PendingFileRenameOperations
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\wextract_cleanup0
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\wextract_cleanup1

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\wextract_cleanup2
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\CLRLoadLogDir
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\.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\Wow6432Node\Microsoft\.NETFramework\AltJit
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_USERS\.DEFAULT\Control Panel\International\LocaleName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Defender\Features\TamperProtection
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableBehaviorMonitoring
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableIOAVProtection
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableOnAccessProtection
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableScanOnRealtimeEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Notifications\DisableNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\AUOptions
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\AutoInstallMinorUpdates
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\NoAutoUpdate
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\NoAutoRebootWithLoggedOnUsers
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\UseWUServer
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\DoNotConnectToWindowsUpdateInternetLocations

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\WUStatusServer
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\WUServer
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\UpdateServiceUrlAlternate
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller\ImagePath
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller\WOW64
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ProgramData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\Public
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\Default
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir (x86)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir (x86)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramW6432Dir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonW6432Dir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-18\ProfileImagePath
HKEY_USERS\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
HKEY_USERS\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Local AppData
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller\Environment
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller\ErrorControl
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller\Tag
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller\DependOnService
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller\DependOnGroup
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller\Group
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\WinDefend\ImagePath
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\WinDefend\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\WinDefend\Start

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\IXP000.TMP\TMP4351$.TMP
C:\Users\user\AppData\Local\Temp\IXP000.TMP\z8784040.exe
C:\Users\user\AppData\Local\Temp\IXP000.TMP\t1498787.exe
C:\Users\user\AppData\Local\Temp\IXP001.TMP\TMP4351$.TMP
C:\Users\user\AppData\Local\Temp\IXP001.TMP\z7869856.exe
C:\Users\user\AppData\Local\Temp\IXP001.TMP\s6358817.exe
C:\Users\user\AppData\Local\Temp\IXP002.TMP\TMP4351$.TMP
C:\Users\user\AppData\Local\Temp\IXP002.TMP\p2889321.exe
C:\Users\user\AppData\Local\Temp\IXP002.TMP\r4984541.exe
C:\Windows\sysnative\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48
C:\Windows\sysnative\LogFiles\Scm\044a6734-e90e-4f8f-b357-b2dc8ab3b5ec
C:\Windows\Logs\CBS\CBS.log

C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenservicelock.dat
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenrootstorelock.dat
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen_service.log
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenofflinequeuelock.dat
C:\Windows\Microsoft.NET\ngenservice_pri3_lock.dat
C:\Windows\Microsoft.NET\ngennicupdatelock.dat
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngenservicelock.dat
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngenrootstorelock.dat
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen_service.log
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngenofflinequeuelock.dat
\??\PIPE\srvsvc
\Device\LanmanDatagramReceiver
\??\SPDevice
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM
C:\Users\user\AppData\Local\CrashDumps\s6358817.exe.2084.dmp
\??\PIPE\wkssvc
C:\Windows\sysnative\winevt\Logs\Microsoft-Windows-Resource-Exhaustion-Resolver%4Operational.evtx
C:\Users\user\AppData\Local\Temp\41bde21dc7\legends.exe

RESOLVED APIS

kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.FlsAlloc
kernel32.dll.FlsSetValue
kernel32.dll.FlsGetValue
kernel32.dll.LCMapStringEx
kernel32.dll.AreFileApisANSI
kernel32.dll.CompareStringEx
kernel32.dll.EnumSystemLocalesEx
kernel32.dll.GetDateFormatEx
kernel32.dll.GetLocaleInfoEx
kernel32.dll.GetTimeFormatEx
kernel32.dll.GetUserDefaultLocaleName
kernel32.dll.IsValidLocaleName
kernel32.dll.LCIDToLocaleName
kernel32.dll.LocaleNameToLCID
kernel32.dll.VirtualProtect
advapi32.dll.GetTokenInformation
advapi32.dll.RegDeleteValueA
advapi32.dll.RegOpenKeyExA
advapi32.dll.RegQueryInfoKeyA
advapi32.dll.FreeSid
advapi32.dll.OpenProcessToken
advapi32.dll.RegSetValueExA

advapi32.dll.RegCreateKeyExA
advapi32.dll.LookupPrivilegeValueA
advapi32.dll.AllocateAndInitializeSid
advapi32.dll.RegQueryValueExA
advapi32.dll.EqualSid
advapi32.dll.RegCloseKey
advapi32.dll.AdjustTokenPrivileges
kernel32.dll._lopen
kernel32.dll._llseek
kernel32.dll.CompareStringA
kernel32.dll.GetLastError
kernel32.dll.GetFileAttributesA
kernel32.dll.GetSystemDirectoryA
kernel32.dll.LoadLibraryA
kernel32.dll.DeleteFileA
kernel32.dll.GlobalAlloc
kernel32.dll.GlobalFree
kernel32.dll.CloseHandle
kernel32.dll.WritePrivateProfileStringA
kernel32.dll.IsDBCSLeadByte
kernel32.dll.GetWindowsDirectoryA
kernel32.dll.SetFileAttributesA
kernel32.dll.GetProcAddress
kernel32.dll.GlobalLock
kernel32.dll.LocalFree
kernel32.dll.RemoveDirectoryA
kernel32.dll.FreeLibrary
kernel32.dll._lclose
kernel32.dll.CreateDirectoryA
kernel32.dll.GetPrivateProfileIntA
kernel32.dll.GetPrivateProfileStringA
kernel32.dll.GlobalUnlock
kernel32.dll.ReadFile
kernel32.dll.SizeofResource
kernel32.dll.WriteFile
kernel32.dll.GetDriveTypeA
kernel32.dll.lstrcmpA
kernel32.dll.SetFileTime
kernel32.dll.SetFilePointer
kernel32.dll.FindResourceA
kernel32.dll.CreateMutexA
kernel32.dll.GetVolumeInformationA

kernel32.dll.ExpandEnvironmentStringsA
kernel32.dll.GetCurrentDirectoryA
kernel32.dll.FreeResource
kernel32.dll.GetVersion
kernel32.dll.SetCurrentDirectoryA
kernel32.dll.GetTempPathA
kernel32.dll.LocalFileTimeToFileTime
kernel32.dll.CreateFileA
kernel32.dll.SetEvent
kernel32.dll.TerminateThread
kernel32.dll.GetVersionExA

DELETED FILES

C:\Users\user\AppData\Local\Temp\IXP000.TMP
C:\Users\user\AppData\Local\Temp\IXP001.TMP
C:\Users\user\AppData\Local\Temp\IXP001.TMP\s6358817.exe
C:\Users\user\AppData\Local\Temp\IXP001.TMP\z7869856.exe
C:\Users\user\AppData\Local\Temp\IXP001.TMP\
C:\Users\user\AppData\Local\Temp\IXP002.TMP
C:\Users\user\AppData\Local\Temp\IXP002.TMP\r4984541.exe
C:\Users\user\AppData\Local\Temp\IXP002.TMP\p2889321.exe
C:\Users\user\AppData\Local\Temp\IXP002.TMP\
C:\Windows\Microsoft.NET\ngenserviceclientlock.dat
C:\Windows\Microsoft.NET\ngenservice_pri0_lock.dat
C:\Windows\Microsoft.NET\ngenservice_pri1_lock.dat
C:\Windows\Microsoft.NET\ngenservice_pri2_lock.dat
C:\Users\user\AppData\Local\CrashDumps\OLLYDBG.EXE.3040.dmp

DELETED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\wextract_cleanup1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\wextract_cleanup2

REGISTRY KEYS

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\PendingFileRenameOperations
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\wextract_cleanup0
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\wextract_cleanup1
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\wextract_cleanup2
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\OnlyUseLatestCLR
Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\Standards\v4.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\v4.0.30319\SKUs\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319\SKUs\client
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Full\Release
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\AppLaunch.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\Wow6432Node\Microsoft\.NETFramework\AltJit
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.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\.NETFramework\Policy\APTCA

HKEY_USERS\S-1-5-18

HKEY_USERS\.DEFAULT\Control Panel\International

HKEY_USERS\.DEFAULT\Control Panel\International\LocaleName

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 Defender\Features

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Defender\Features\TamperProtection

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableBehaviorMonitoring

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableIOAVProtection

EXECUTED COMMANDS

C:\Users\user\AppData\Local\Temp\IXP000.TMP\z8784040.exe

C:\Users\user\AppData\Local\Temp\IXP000.TMP\t1498787.exe

C:\Users\user\AppData\Local\Temp\IXP001.TMP\z7869856.exe

C:\Users\user\AppData\Local\Temp\IXP001.TMP\s6358817.exe

C:\Users\user\AppData\Local\Temp\IXP002.TMP\p2889321.exe

C:\Users\user\AppData\Local\Temp\IXP002.TMP\r4984541.exe

C:\Windows\servicing\TrustedInstaller.exe

C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe

C:\Windows\system32\sppsvc.exe

C:\Windows\System32\svchost.exe -k WerSvcGroup

C:\Windows\system32\sc.exe start w32time task_started

C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding

\\?\C:\Windows\system32\wbem\WMIADAP.EXE wmiadap.exe /F /T /R

C:\Windows\SysWOW64\WerFault.exe -u -p 2084 -s 1012

C:\Users\user\AppData\Local\Temp\41bde21dc7\legends.exe

READ FILES

C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe.config
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
C:\Windows\System32\MSVCR120_CLR0400.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config
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\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
\Device\KsecDD
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll
C:\Windows\assembly\pubpol20.dat
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\Microsoft.NET\Framework\v4.0.30319\nlssorting.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\SortDefault.nlp
C:\Windows\sysnative\LogFiles\Scm\044a6734-e90e-4f8f-b357-b2dc8ab3b5ec
C:\Windows\Logs\CBS\CBS.log
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Users\user\AppData\Local\Temp\IXP002.TMP\r4984541.exe.config
C:\Users\user\AppData\Local\Temp\IXP002.TMP\r4984541.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
C:\Windows\sysnative\MSVCR120_CLR0400.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\fa8eef6f6cb67c660d71e15c5cad71b5\mscorlib.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\fa8eef6f6cb67c660d71e15c5cad71b5\mscorlib.ni.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clrjit.dll
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\5f665a4076cb8d9479ca406e7827fb9f\System.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\5f665a4076cb8d9479ca406e7827fb9f\System.ni.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\nlssorting.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SortDefault.nlp
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\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\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\System32\tzres.dll

C:\Windows\System32\en-US\tzres.dll.mui
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\4695703083096416564b52b0696c5d9\System.Configuration.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\4695703083096416564b52b0696c5d9\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.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.aux
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.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:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvc.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\fusion.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen_service.log
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe.config
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
C:\Windows\assembly\GAC_MSIL\Accessibility\2.0.0.0__b03f5f7f11d50a3a\Accessibility.dll.config
C:\Windows\assembly\GAC_MSIL\Accessibility\2.0.0.0__b03f5f7f11d50a3a\Accessibility.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\AspNetMMCExt\v4.0_4.0.0.0__b03f5f7f11d50a3a\AspNetMMCExt.dll.config
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\AspNetMMCExt\v4.0_4.0.0.0__b03f5f7f11d50a3a\AspNetMMCExt.dll
C:\Windows\assembly\GAC_32\AuditPolicyGPManagedStubs.Interop\6.1.0.0__31bf3856ad364e35\AuditPolicyGPManagedStubs.Interop.dll.config
C:\Windows\assembly\GAC_32\AuditPolicyGPManagedStubs.Interop\6.1.0.0__31bf3856ad364e35\AuditPolicyGPManagedStubs.Interop.dll
C:\Windows\assembly\GAC_32\BDATunePIA\6.1.0.0__31bf3856ad364e35\BDATunePIA.dll.config

MUTEXES

Global\WdsSetupLogInit
Global\SetupLog
Local\WERReportingForProcess2084
Global\e31afbb3-1503-11ee-89ac-08002723e461
Global\ADAP_WMI_ENTRY
Global\RefreshRA_Mutex
Global\RefreshRA_Mutex_Lib

Global\RefreshRA_Mutex_Flag
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

STARTED SERVICES

TrustedInstaller
WerSvc

MODIFIED REGISTRY KEYS

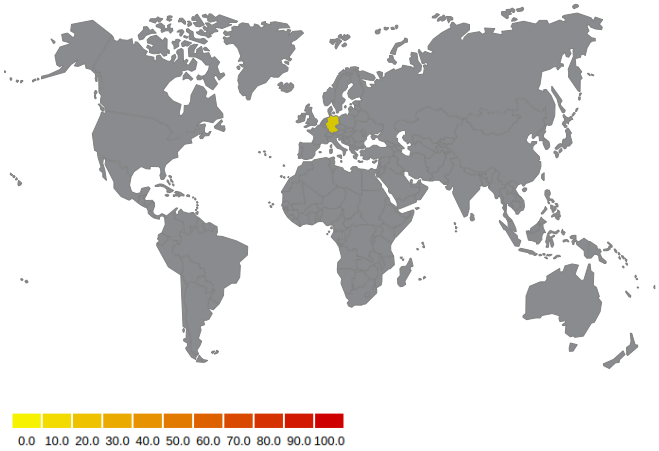
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\wextract_cleanup0
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\wextract_cleanup1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\wextract_cleanup2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Features
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Defender\Features\TamperProtection
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableBehaviorMonitoring
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableIOAVProtection
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableOnAccessProtection
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableScanOnRealtimeEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Notifications
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Notifications\DisableNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\AUOptions
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\AutoInstallMinorUpdates
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\NoAutoUpdate
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\NoAutoRebootWithLoggedOnUsers
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\UseWUServer
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\DoNotConnectToWindowsUpdateInternetLocations
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\WinDefend\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\wuauserv\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v4.0.30319_32\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Winmgmt\Type
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v4.0.30319_64\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\WerSvc\Type
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Features\TamperProtection
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Accessibility, Version=2.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\AspNetMMCExt, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\AuditPolicyGPManagedStubs.Interop, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=x86\1\RuntimeVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\BDATunePIA, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=x86\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/aspnet_intern.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/aspnet_merge.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/AxImp.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/lc.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/ResGen.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/SecAnnotate.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/sgen.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/SqlMetal.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/SvcUtil.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/TlbExp.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/TlbImp.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/WinMDExp.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/wsdl.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/xsd.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Program Files (x86)/Microsoft SDKs/Windows/v8.1A/bin/NETFX 4.5.1 Tools/xsltc.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Windows/Microsoft.NET/Framework/v4.0.30319/ComSvcConfig.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Windows/Microsoft.NET/Framework/v4.0.30319/dfsvc.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Windows/Microsoft.NET/Framework/v4.0.30319/MSBuild.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Windows/Microsoft.NET/Framework/v4.0.30319/SMSvcHost.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\C:/Windows/Microsoft.NET/Framework/v4.0.30319/WsatConfig.exe\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\ComSvcConfig, Version=3.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\CustomMarshalers, Version=2.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=x86\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\dfsvc, Version=2.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\ehexthost32, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=x86\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\ehiExtens, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\EventViewer, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\mcstoredb, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=x86\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Activities.Build, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.ApplicationId.Framework, Version=6.1.0.0, Culture=Neutral, PublicKeyToken=31bf3856ad364e35, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.ApplicationId.RuleWizard, Version=6.1.0.0, Culture=Neutral,

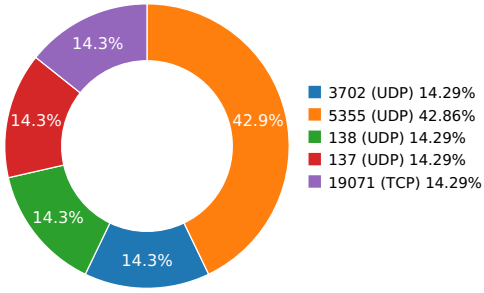
PublicKeyToken=31bf3856ad364e35, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Conversion.v3.5, Version=3.5.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Conversion.v4.0, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Engine, Version=2.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Engine, Version=3.5.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Engine, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Framework, Version=2.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Framework, Version=3.5.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Framework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a\0\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Tasks, Version=2.0.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Tasks.v3.5, Version=3.5.0.0, Culture=Neutral, PublicKeyToken=b03f5f7f11d50a3a, processorArchitecture=msil\1\RuntimeVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727\NGENService\Roots\Microsoft.Build.Tasks.v4.0, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a\0\RuntimeVersion

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	83.97.73.128	Germany	208312	Not known	Malware Process

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
66.065456152	Sandbox	83.97.73.128	19071

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.12611317635	Sandbox	224.0.0.252	5355
3.12861800194	Sandbox	192.168.56.255	137
3.17031502724	Sandbox	224.0.0.252	5355
3.1838350296	Sandbox	239.255.255.250	3702
5.73814105988	Sandbox	224.0.0.252	5355
9.26638412476	Sandbox	192.168.56.255	138

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\IXP001.TMP\Z7869856.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** e2e1fa6fb24d597c4baba91aaeed2053 **SHA-1 :** e53d60465e459a7a643d01d6fd13a6b09cf4c4e4 **SHA-256 :** e6e7ad43a309c948700ed0dd81c8177572cabb0d39b62c61383 **SHA-512 :** dc80d75d92ac7a4706dbd27ff02023ff9d85d737681cbf67f37ce4 **Size :** 232.448 Kilobytes.
C:\Users\User\AppData\Local\Temp\IXP002.TMP\P2889321.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 211a06e9ae68ced1234252a48696431b **SHA-1 :** 69950e2ee2fafd177d1a295836713bfd8d18df9c **SHA-256 :** 0bdca9c84103454e329cfde4e69dc41a0ec0196c078c8fc195b0f **SHA-512 :** b1643ba376075619335b4bdf0d7610aece13b7c9db60eecb508 **Size :** 180.544 Kilobytes.
C:\Users\User\AppData\Local\Temp\IXP001.TMP\S6358817.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** 0ff113c12c86ad2f2110879308c95299 **SHA-1 :** 19ec931c74772cf3dfe1bb35e82be3c3b096cfd7 **SHA-256 :** 6dc9965a8b6eee21a4ef6c86c2df2973c170818da401a7ef13f72 **SHA-512 :** da894d0a7270b55d370b5615ae9db164a3d1a026ae80f9cc22ac **Size :** 397.824 Kilobytes.
C:\Users\User\AppData\Local\Temp\IXP002.TMP\R4984541.Exe	**Type :** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 7e93bacbbc33e6652e147e7fe07572a0 **SHA-1 :** 421a7167da01c8da4dc4d5234ca3dd84e319e762 **SHA-256 :** 850cd190aaeebcf1505674d97f51756f325e650320eaf76785d95 **SHA-512 :** 250169d7b6fcebff400be89edae8340f14130ced70c340ba9da9f **Size :** 11.264 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	bdbdc0e68f0175414075ae9841781c51ce3784d7
File Type:	PE32 executable (console) Intel 80386, for MS Windows
SHA1:	bdbdc0e68f0175414075ae9841781c51ce3784d7
MD5:	a494133a749128886cf99016e767f5dc
First Seen Date:	2023-06-27 15:20:35.051858 (3 months ago)
Number Of Clients Seen:	6
Last Analysis Date:	2023-06-27 16:57:11.732198 (3 months ago)
Human Expert Analysis Date:	2023-06-28 08:12:19.396679 (3 months ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	1
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	6
Trid	[[67.4, u'Win32 Executable MS Visual C++ (generic)'], [14.2, u'Win32 Dynamic Link Library (generic)'], [9.7, u'Win32 Executable (generic)'], [4.3, u'Generic Win/DOS Executable'], [4.3, u'DOS Executable Generic']]
Compilation Time Stamp	0x64939328 [Thu Jun 22 00:17:44 2023 UTC]
LegalCopyright	\xa9 Macquarie Group Limited All rights reserved.
InternalName	eDqzdMMvBPnL
FileVersion	754
CompanyName	Macquarie Group Limited
LegalTrademarks	\xa9 Macquarie Group Limited Trademarks
Comments	This is a legitimate application.
ProductName	OVcuX7qJaY
ProductVersion	754
FileDescription	Macquarie Group Limited Product
OriginalFilename	EvQFMQh1.exe
Translation	0x0407 0x04b0
Entry Point	0x40b1ff (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	896512
Ssdeep	12288:scztKepjWeeIOw6IDWJSn/hTUZvLglRPgc70qvSyfrZiaMr4bLHYN9YbUJOqqKbS:dkNeemn/MDgSxqvSyfonsb0NmrQb8j
Sha256	427875607eaf3406b8a2212e6a4671bf6ded47f771f2bd39228014d05954214f
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/b/d/b/d/bdbdc0e68f0175414075ae9841781c51ce3784d7', u'EXE:OriginalFileName': u'EvQFMQh1.exe', u'EXE:ProductName': u'OVcuX7qJaY', u'EXE:InternalName': u'eDqzdMMvBPnL', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2023:06:27 15:20:16+00:00', u'EXE:InitializedDataSize': 740864, u'File:FileModifyDate': u'2023:06:22 06:42:56+00:00', u'EXE:FileVersionNumber': u'754.0.0.0', u'EXE:FileVersion': 754, u'File:FileSize': u'876 kB', u'EXE:CharacterSet': u'Windows, Latin1', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:LegalTrademarks': u'\xa9 Macquarie Group Limited Trademarks', u'EXE:ProductVersion': 754, u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'Macquarie Group Limited', u'File:FileName': u'bdbdc0e68f0175414075ae9841781c51ce3784d7', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 6.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2023:06:22 00:17:44+00:00', u'EXE:FileFlagsMask': u'0x0000', u'EXE:LegalCopyright': u'\xa9 Macquarie Group Limited All rights reserved.', u'EXE:LinkerVersion': 14.36, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows command line', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/b/d/b/d', u'EXE:FileDescription': u'Macquarie Group Limited Product', u'EXE:EntryPoint': u'0xb1ff', u'EXE:SubsystemVersion': 6.0, u'EXE:CodeSize': 158208, u'EXE:Comments': u'This is a legitimate application.', u'File:FileInodeChangeDate': u'2023:06:22 06:42:57+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'754.0.0.0'}]
Mime Type	application/x-dosexec
Imphash	5546d5d08c85c9bfc72c6e57a660ba00

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.bqwazg	0x1000	0x1f77	0x2000	6.76477683259	67bfd78e0a83f4d0928fa878c4ee4439
.text	0x3000	0x249b5	0x24a00	6.59492365864	ebbd22b2556e80b89071865b2b9c3dd8
.rdata	0x28000	0xd818	0xda00	5.51858453698	b4d48dda5891246fa03c9b08e01e688b
.data	0x36000	0x1d50	0x1000	3.08126538072	b1153975ff168f41b4ca583f93fd23af
.bqazz	0x38000	0xa4ed0	0xa5000	7.88130267087	7b5314ba8f04e6230940c720c79051c2
.rsrc	0xdd000	0x458	0x600	2.57638045513	c897a9f150f2e42da68002e7e5f4e13d

PE Imports

- KERNEL32.dll
  - WaitForSingleObject
  - Sleep
  - GetCurrentProcess
  - CreateThread
  - GetVersion
  - VirtualAlloc
  - VirtualProtect
  - GetModuleHandleA
  - GetProcAddress
  - LoadLibraryA
  - lstrlenW
  - FreeConsole
  - CreateFileW
  - WideCharToMultiByte
  - EnterCriticalSection
  - LeaveCriticalSection
  - InitializeCriticalSectionEx
  - DeleteCriticalSection
  - EncodePointer
  - DecodePointer
  - MultiByteToWideChar
  - LCMapStringEx
  - GetStringTypeW
  - GetCPInfo
  - IsProcessorFeaturePresent
  - QueryPerformanceCounter
  - GetCurrentProcessId
  - GetCurrentThreadId
  - GetSystemTimeAsFileTime
  - InitializeSListHead
  - IsDebuggerPresent
  - UnhandledExceptionFilter
  - SetUnhandledExceptionFilter
  - GetStartupInfoW
  - GetModuleHandleW
  - TerminateProcess
  - RaiseException
  - RtlUnwind
  - GetLastError
  - SetLastError
  - InitializeCriticalSectionAndSpinCount
  - TlsAlloc
  - TlsGetValue
  - TlsSetValue
  - TlsFree
  - FreeLibrary
  - LoadLibraryExW
  - GetStdHandle
  - WriteFile
  - GetModuleFileNameW
  - ExitProcess
  - GetModuleHandleExW
  - GetCommandLineA
  - GetCommandLineW
  - HeapAlloc
  - HeapFree
  - GetFileType
  - CompareStringW
  - LCMapStringW
  - GetLocaleInfoW
  - IsValidLocale
  - GetUserDefaultLCID
  - EnumSystemLocalesW
  - CloseHandle
  - FlushFileBuffers
  - GetConsoleOutputCP
  - GetConsoleMode
  - ReadFile
  - GetFileSizeEx
  - SetFilePointerEx
  - ReadConsoleW
  - HeapReAlloc
  - FindClose

- FindFirstFileExW
- FindNextFileW
- IsValidCodePage
- GetACP
- GetOEMCP
- GetEnvironmentStringsW
- FreeEnvironmentStringsW
- SetEnvironmentVariableW
- SetStdHandle
- GetProcessHeap
- HeapSize
- WriteConsoleW

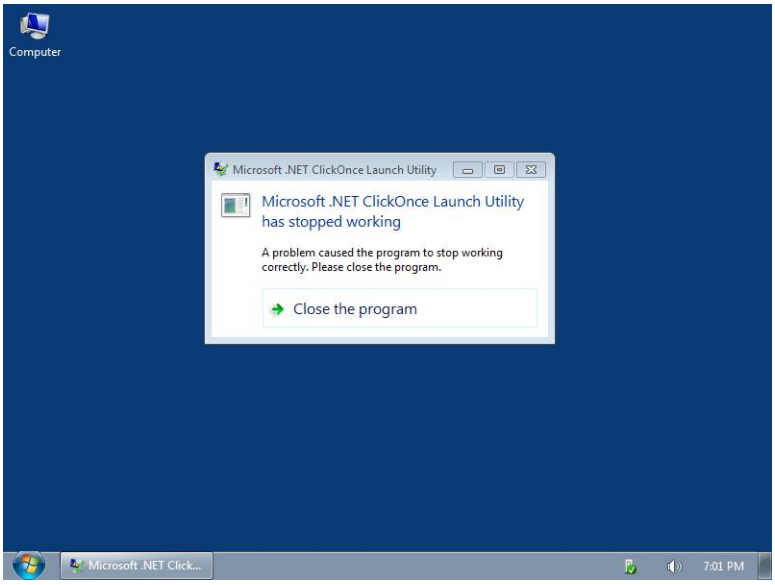
PE Resources

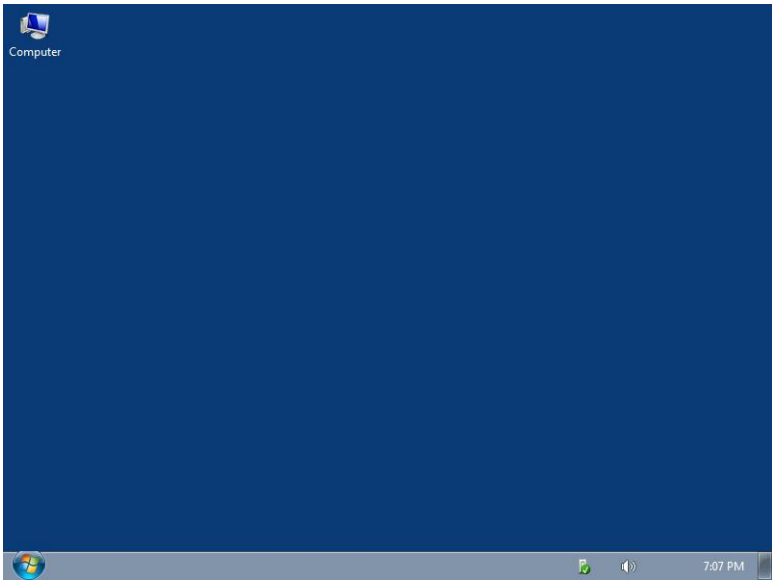
{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 905312, u'sha256': u'f5f59d3e9739f7623285f14305091fea2a8c3c68195487853d7eeeb805bcc8d6', u'type': u'data', u'size': 1012}

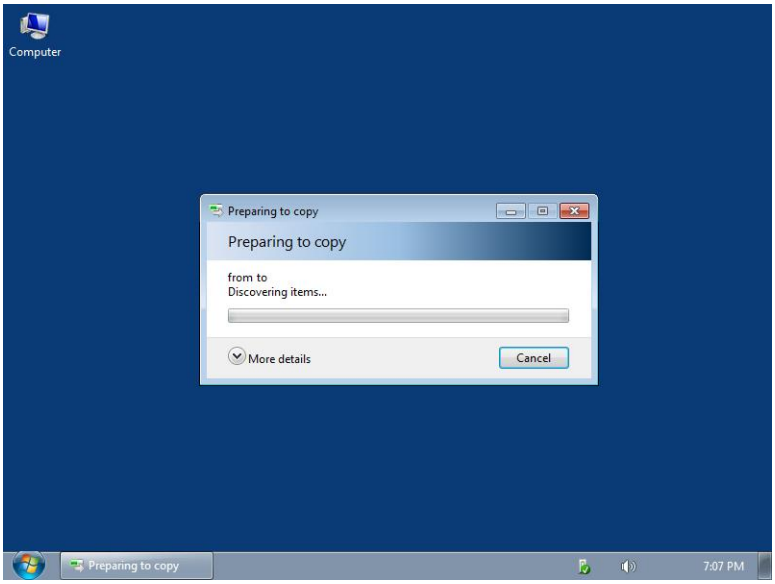
CERTIFICATE VALIDATION

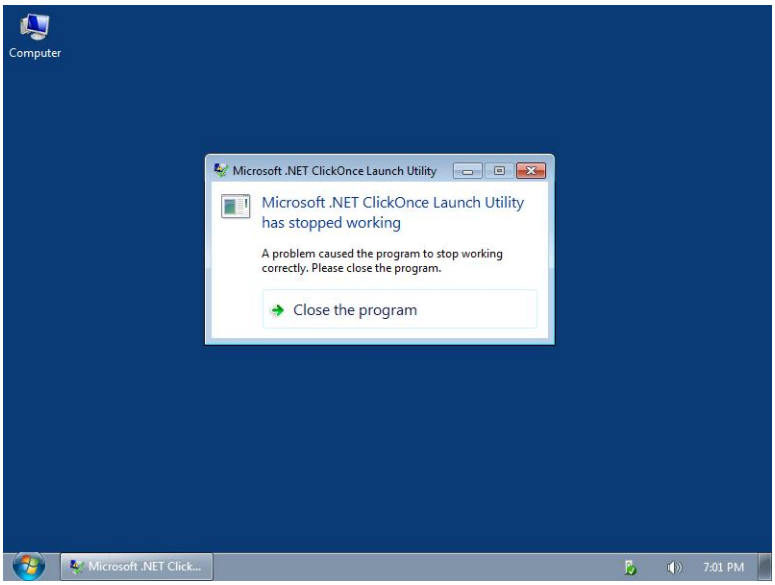
- Certificate Validation is not Applicable ?

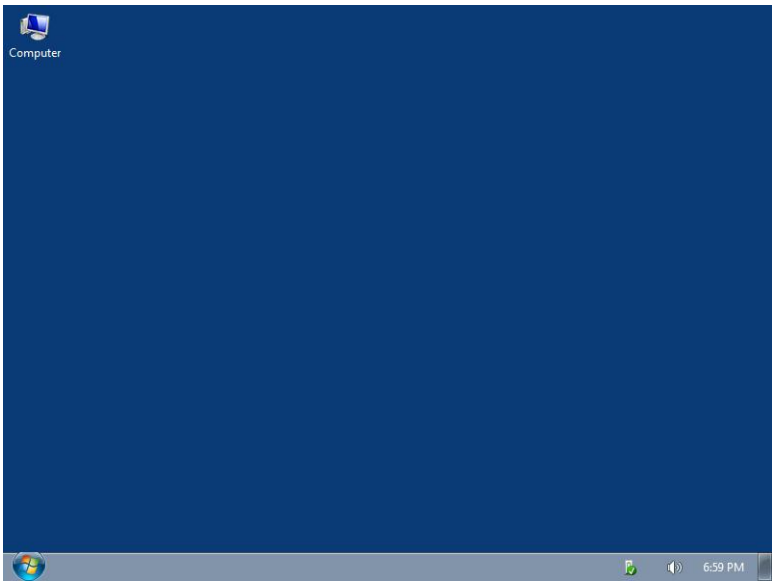
SCREENSHOTS

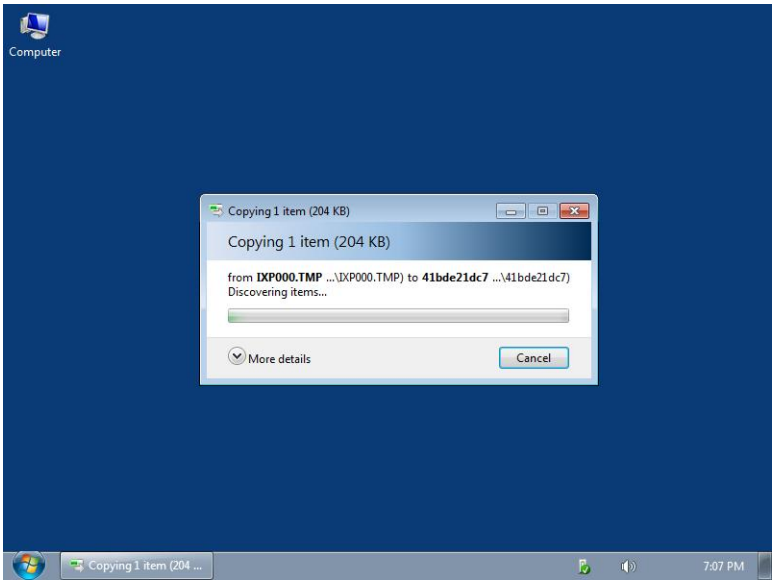


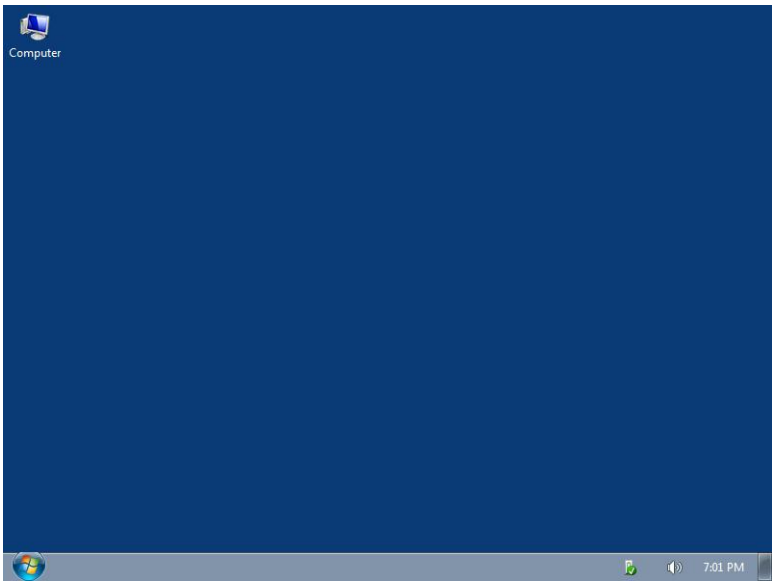



Computer
Preparing to copy
Preparing to copy
from to
Discovering items...
More details
Cancel
Preparing to copy
7:07 PM


Computer
Microsoft .NET ClickOnce Launch Utility
Microsoft .NET ClickOnce Launch Utility has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
Microsoft .NET Click...
7:01 PM


Computer
6:59 PM


Computer
Copying 1 item (204 KB)
Copying 1 item (204 KB)
from IXP000.TMP ...\IXP000.TMP) to 41bde21dc7 ...\41bde21dc7)
Discovering items...
More details
Cancel
Copying 1 item (204 ...
7:07 PM


Computer
7:01 PM