

Summary

File Name: 29c8d201060f864bd41f4c57c767241e2f57ea9b

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

SHA1: 29c8d201060f864bd41f4c57c767241e2f57ea9b

MD5: e00521e507bc8e874d98c2218423180a

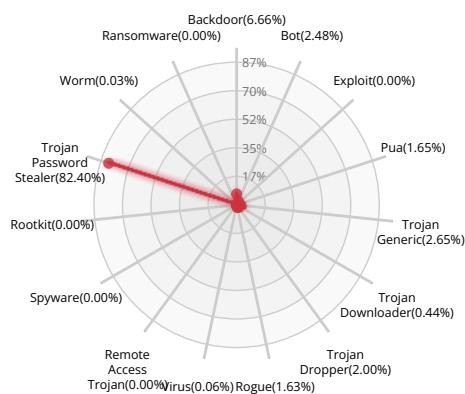


Xcitium Verdict Cloud Final
Verdict

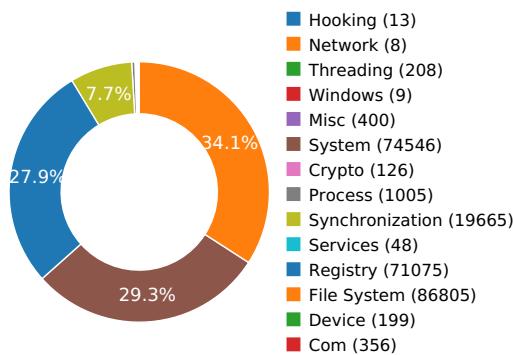
DETECTION SECTION



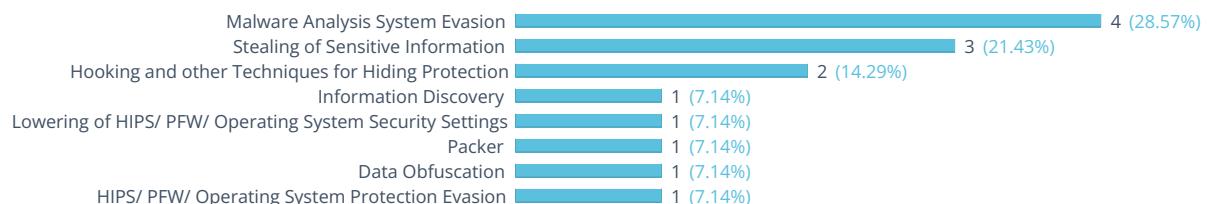
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



Activity Details

INFORMATION DISCOVERY



Reads data out of its own binary image

Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS



Attempts to block SafeBoot use by removing registry keys

Show sources

PACKER



The binary likely contains encrypted or compressed data.

Show sources

STEALING OF SENSITIVE INFORMATION



Steals private information from local Internet browsers

Show sources

Harvests credentials from local FTP client softwares

Show sources

Harvests information related to installed mail clients

Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION



Creates RWX memory

Show sources

Executed a process and injected code into it, probably while unpacking

Show sources

DATA OBFUSCATION



Attempts to execute a powershell command with suspicious parameter/s

Show sources

MALWARE ANALYSIS SYSTEM EVASION



A process attempted to delay the analysis task.

Show sources

Detects VirtualBox through the presence of a file

Show sources

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

Show sources

Creates a hidden or system file

Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

Attempts to identify installed AV products by installation directory

Show sources

Behavior Graph

04:37:49

04:41:03

04:44:17

PID 2360

04:37:49

Create Process

The malicious file created a child process as 29c8d201060f864bd41f4c57c767241e2f57ea9b.exe (**PPID 2312**)

04:37:49 VirtualProtectEx

04:37:50 NtDelayExecution

04:38:01 NtSetInformationFile

04:38:02 CreateProcessInternal

04:38:02 Create Process

04:38:06 Create Process

04:38:06 Create Process

04:38:06 Create Process

04:38:06 Create Process

04:38:07 Create Process

04:38:07 NtResumeThread

PID 2496

04:38:03

Create Process

The malicious file created a child process as powershell.exe (**PPID 2360**)

04:38:03 NtQueryFullAttributesFile [12 times]

PID 3004

04:38:10

Create Process

The malicious file created a child process as 29c8d201060f864bd41f4c57c767241e2f57ea9b.exe (**PPID 2360**)

04:38:26 NtReadFile [11 times]

04:43:50 Create Process

PID 1044

04:44:13

Create Process

The malicious file created a child process as WerFault.exe (**PPID 3004**)

PID 2536

04:38:04

Create Process

The malicious file created a child process as schtasks.exe (**PPID 2360**)

PID 880

04:38:05

Create Process

The malicious file created a child process as svchost.exe (**PPID 460**)

PID 460

04:38:49

Create Process

The malicious file created a child process as services.exe (**PPID 352**)

04:38:50 Create Process

04:39:25 Create Process

04:39:32 Create Process

04:39:46 Create Process

04:40:17 Create Process

04:41:59
04:44:17 GetSystemTimeAsFileTime [47 times]

04:43:20 Create Process

PID 2960

04:38:51

Create ProcessThe malicious file created a child process as lsass.exe (**PPID 460**)**PID 1996**

04:39:30

Create ProcessThe malicious file created a child process as mscorsvw.exe (**PPID 460**)**PID 2500**

04:39:36

Create ProcessThe malicious file created a child process as mscorsvw.exe (**PPID 460**)**PID 2836**

04:39:48

Create ProcessThe malicious file created a child process as sppsvc.exe (**PPID 460**)

04:42:30

RegOpenKeyExW**PID 1584**

04:40:09

Create ProcessThe malicious file created a child process as taskhost.exe (**PPID 460**)**PID 568**

04:43:30

Create ProcessThe malicious file created a child process as svchost.exe (**PPID 460**)**PID 644**

04:43:46

Create ProcessThe malicious file created a child process as VBoxService.exe (**PPID 460**)**PID 468**

04:42:40

Create ProcessThe malicious file created a child process as lsass.exe (**PPID 352**)

Behavior Summary

ACCESSED FILES

C:\Windows\System32\MSCOREE.DLL.local
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework*
C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll
C:\Windows\Microsoft.NET\Framework\v1.0.3705\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v1.1.4322\clr.dll
C:\Windows\Microsoft.NET\Framework\v1.1.4322\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
C:\Users\user\AppData\Local\Temp\29c8d201060f864bd41f4c57c767241e2f57ea9b.exe.config
C:\Users\user\AppData\Local\Temp\29c8d201060f864bd41f4c57c767241e2f57ea9b.exe
C:\Users\user\AppData\Local\Temp\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\System32\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\system\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\ProgramData\Oracle\Java\javapath\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\System32\wbem\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Universal Extractor\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Python27\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Python27\Scripts\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\sysinternals\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\IDA_Pro_v6\python\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\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\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:\Users

C:\Users\user

C:\Users\user\AppData

C:\Users\user\AppData\Local

C:\Users\user\AppData\Local\Temp

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

\Device\KsecDD

C:\Windows\Assembly\NativeImages_v4.0.30319_32\gPUB*

C:\Users\user\AppData\Local\Temp\29c8d201060f864bd41f4c57c767241e2f57ea9b.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.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

C:\Windows\Assembly\NativeImages_v4.0.30319_32\System.Drawing*

C:\Windows\Assembly\NativeImages_v4.0.30319_32\System.Drawing\646b4b01cb29986f8e076aa65c9e9753\System.Drawing.ni.dll

C:\Windows\Assembly\NativeImages_v4.0.30319_32\System.Drawing\646b4b01cb29986f8e076aa65c9e9753\System.Drawing.ni.dll.aux

C:\Windows\Microsoft.Net\Assembly\GAC_MSIL\System.Security\v4.0_4.0.0.0_b03f5f7f11d50a3a\System.Security.dll

C:\Windows\Microsoft.Net\Assembly\GAC_MSIL\Accessibility\v4.0_4.0.0.0_b03f5f7f11d50a3a\Accessibility.dll

C:\Windows\Microsoft.Net\Assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0_b77a5c561934e089\System.Core.dll

C:\Windows\Microsoft.Net\Assembly\GAC_MSIL\System.Deployment\v4.0_4.0.0.0_b03f5f7f11d50a3a\System.Deployment.dll

C:\Windows\Microsoft.Net\Assembly\GAC_MSIL\System.Runtime.Serialization.Formatters.Soap\v4.0_4.0.0.0_b03f5f7f11d50a3a\System.Runtime.Serialization.Formatters.Soap.dll

C:\Windows\Microsoft.Net\Assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0_b77a5c561934e089\uxtheme.dll

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

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

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

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\InstallRoot

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\CLRLoadLogDir

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\OnlyUseLatestCLR

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Fusion\NoClientChecks

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\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\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US

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_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest

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\.NETFramework\DbgJITDebugLaunchSetting

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DbgManagedDebugger

HKEY_CURRENT_USER\Software\Microsoft\GDIPlus\FontCachePath

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{031E4825-7B94-4dc3-B131-E946B44C8DD5\}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{04731B67-D933-450a-90E6-4ACD2E9408FE\}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{11016101-E366-4D22-BC06-4ADA335C892B\}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{26EE0668-A00A-44D7-9371-BEB064C98683\}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{4336a54d-038b-4685-ab02-99bb52d3fb8b\}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{450D8FBA-AD25-11D0-98A8-0800361B1103\}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0\}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{645FF040-5081-101B-9F08-00AA002F954E}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{89D83576-6BD1-4c86-9454-BEB04E94C819}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{9343812e-1c37-4a49-a12e-4b2d810d956b}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{B4FB3F98-C1EA-428d-A78A-D1F5659CBA93}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{BD7A2E7B-21CB-41b2-A086-B309680C6B7E}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{daf95313-e44d-46af-be1b-cbacea2c3065}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{e345f35f-9397-435c-8f95-4e922c26259e}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{ED228FDF-9EA8-4870-83b1-96b02CFE0D52}\SuppressionPolicy

MODIFIED FILES

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

C:\Users\user\AppData\Roaming\NionjZ.exe

C:\Users\user\AppData\Local\Temp\tmpF03C.tmp

C:\Users\user\AppData\Local\Temp%\ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk

\??\PIPE\srvsvc

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\ZLA30G1THTOMCCZR1LRJ.temp

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms

C:\Windows\sysnative\Tasks\Updates\NionjZ

C:\Windows\Temp\fwtssqlmfile00.sqm

\Device\LanmanDatagramReceiver

\??\pipe\PIPE_EVENTROOT\CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER

\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM

C:\Windows\WindowsUpdate.log

C:\Windows\sysnative\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fd62c48

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\ngenofflinequeueunlock.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\ngenofflinequeueunlock.dat

\??\SPDevice

RESOLVED APIs

advapi32.dll.RegOpenKeyExW

advapi32.dll.RegQueryInfoKeyW

advapi32.dll.RegEnumKeyExW

advapi32.dll.RegEnumValueW

advapi32.dll.RegCloseKey

advapi32.dll.RegQueryValueExW

kernel32.dll.FlsAlloc

kernel32.dll.FlsFree

kernel32.dll.FlsGetValue

kernel32.dll.FlsSetValue

kernel32.dll.InitializeCriticalSectionEx

kernel32.dll.CreateEventExW

kernel32.dll.CreateSemaphoreExW

kernel32.dll.SetThreadStackGuarantee

kernel32.dll.CreateThreadpoolTimer

kernel32.dll.SetThreadpoolTimer

kernel32.dll.WaitForThreadpoolTimerCallbacks

kernel32.dll.CloseThreadpoolTimer

kernel32.dll.CreateThreadpoolWait

kernel32.dll.SetThreadpoolWait

kernel32.dll.CloseThreadpoolWait

kernel32.dll.FlushProcessWriteBuffers

kernel32.dll.FreeLibraryWhenCallbackReturns

kernel32.dll.GetCurrentProcessorNumber

kernel32.dll.GetLogicalProcessorInformation

kernel32.dll.CreateSymbolicLinkW

kernel32.dll.EnumSystemLocalesEx

kernel32.dll.CompareStringEx

kernel32.dll.GetDateFormatEx

kernel32.dll.GetLocaleInfoEx

kernel32.dll.GetTimeFormatEx

kernel32.dll.GetUserDefaultLocaleName

kernel32.dll.IsValidLocaleName

kernel32.dll.LCMapStringEx

kernel32.dll.GetTickCount64

advapi32.dll.EventRegister

mscoree.dll.#142

mscoreei.dll.RegisterShimImplCallback

mscoreei.dll.OnShimDIIIMainCalled

mscoreei.dll._CorExeMain

shlwapi.dll.UrlIsW

version.dll.GetFileVersionInfoSizeW

version.dll.GetFileVersionInfoW

version.dll.VerQueryValueW

clr.dll.SetRuntimeInfo

clr.dll._CorExeMain

mscoree.dll.CreateConfigStream

mscoreei.dll.CreateConfigStream

kernel32.dll.GetNumaHighestNodeNumber

kernel32.dll.GetSystemWindowsDirectoryW

advapi32.dll.AllocateAndInitializeSid

advapi32.dll.OpenProcessToken

advapi32.dll.GetTokenInformation

advapi32.dll.InitializeAcl

advapi32.dll.AddAccessAllowedAce

advapi32.dll.FreeSid

kernel32.dll.AddSIDToBoundaryDescriptor

kernel32.dll.CreateBoundaryDescriptorW

kernel32.dll.CreatePrivateNamespaceW

kernel32.dll.OpenPrivateNamespaceW

kernel32.dll.DeleteBoundaryDescriptor

kernel32.dll.WerRegisterRuntimeExceptionModule

kernel32.dll.RaiseException

mscoree.dll.#24

mscoreei.dll.#24

ntdll.dll.NtSetSystemInformation

kernel32.dll.SortGetHandle

kernel32.dll.SortCloseHandle

kernel32.dll.GetNativeSystemInfo

ole32.dll.CoInitializeEx

cryptbase.dll.SystemFunction036

uxtheme.dll.ThemeInitApiHook

user32.dll.IsProcessDPIAware

ole32.dll.CoGetContextToken

clrjit.dll.sxsJitStartup

clrjit.dll.getJit

DELETED FILES

C:\Users\user\AppData\Local\Temp\tmpF03C.tmp

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\ZLA30G1THTOMCCZR1LRJ.temp

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.2496.12083515

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.2496.12083515

C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2496.12083515

C:\Windows\Microsoft.NET\ngenserviceclientlock.dat

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\v4.0

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\InstallRoot

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\CLRLoadLogDir

HKEY_CURRENT_USER\Software\Microsoft\.NETFramework

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\OnlyUseLatestCLR

Policy\Standards

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\Standards

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\Standards\v4.0.30319

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\default

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\29c8d201060f864bd41f4c57c767241e2f57ea9b.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\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\Software\Microsoft\StrongName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLEAUT
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.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\APTC
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
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

EXECUTED COMMANDS

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\NionjZ.exe"
powershell Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\NionjZ.exe"
schtasks.exe /Create /TN "Updates\NionjZ" /XML "C:\Users\user\AppData\Local\Temp\tmpF03C.tmp"
C:\Windows\SysWOW64\WerFault.exe -u -p 3004 -s 1048
C:\Windows\system32\lsass.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 netsvcs

READ FILES

C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Users\user\AppData\Local\Temp\29c8d201060f864bd41f4c57c767241e2f57ea9b.exe.config
C:\Users\user\AppData\Local\Temp\29c8d201060f864bd41f4c57c767241e2f57ea9b.exe
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\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
\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.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\Assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0_b77a5c561934e089\System.Windows.Forms.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\nlssorting.dll
C:\Windows\Microsoft.NET\Framework\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\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
C:\Windows\Fonts\tahoma.ttf
C:\Windows\Fonts\msjh.ttf
C:\Windows\Fonts\msyh.ttf
C:\Windows\Fonts\malgun.ttf
C:\Windows\Fonts\micross.ttf
C:\Windows\Fonts\segoeui.ttf
C:\Windows\Fonts\staticcache.dat
C:\Windows\Fonts\segoeuib.ttf
C:\Windows\Fonts\segoeuif.ttf
C:\Windows\Fonts\segoeuiz.ttf
C:\Windows\Fonts\seguisb.ttf
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorrc.dll
C:\Windows\Assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\7ca6a7b9413844e82108a9d62f88a2d9\Microsoft.VisualBasic.ni.dll.aux
C:\Windows\Assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\7ca6a7b9413844e82108a9d62f88a2d9\Microsoft.VisualBasic.ni.dll
C:\Windows\SysWOW64\shell32.dll
C:\Windows\SysWOW64\ieframe.dll
C:\
C:\Windows
C:\Windows\System32
C:\Windows\System32\WindowsPowerShell
C:\Windows\System32\WindowsPowerShell\v1.0

C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000004c.db
C:\Users\user\Desktop\desktop.ini
C:\Users\user\AppData\Local\Temp\tmpF03C.tmp
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\ProgramData
C:\ProgramData\Microsoft\desktop.ini
C:\ProgramData\Microsoft
C:\ProgramData\Microsoft\Windows
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\Public\desktop.ini
C:\Users\Public
C:\Users\Public\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch
C:\Windows\System32\shdocvw.dll
C:\Windows\AppPatch\sysmain.sdb

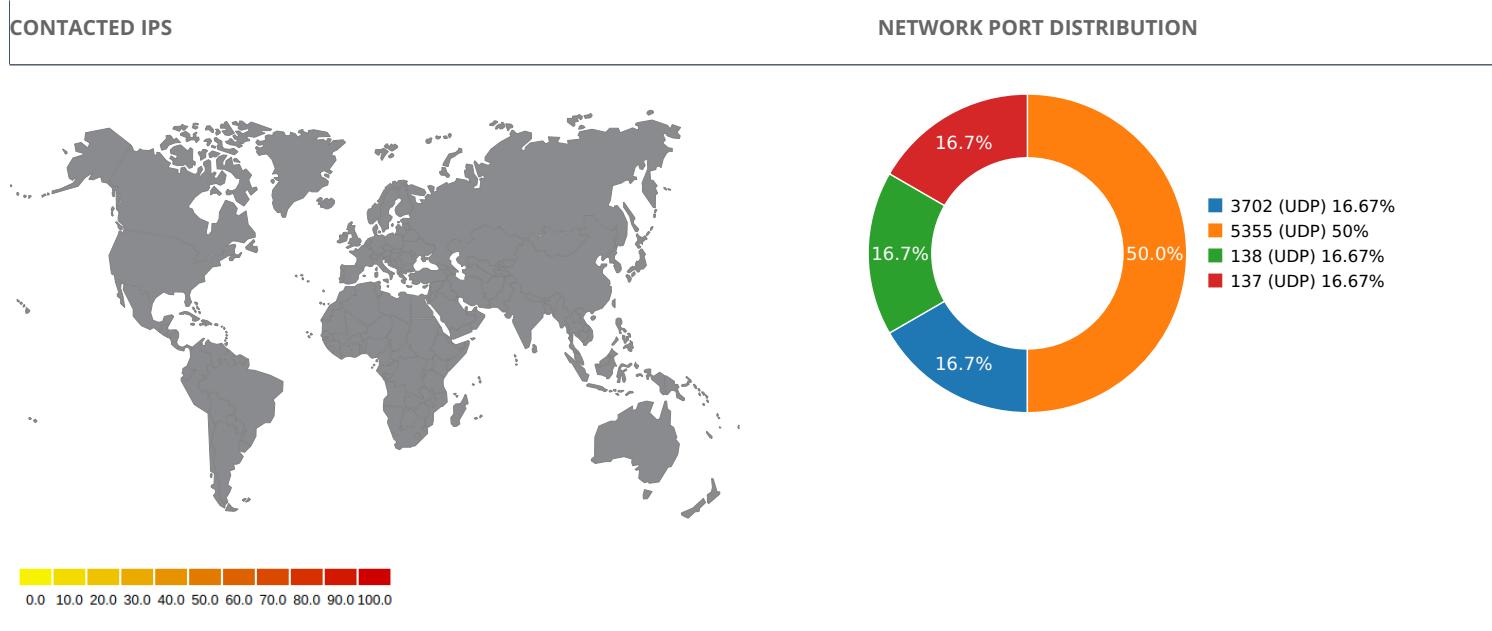
MUTEXES

Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
Global\CLR_CASOFF_MUTEX
Global\WindowsUpdateTracingMutex
DBWinMutex

MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{8ECD3971-5904-4747-A164-F005E421259E}\Path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{8ECD3971-5904-4747-A164-F005E421259E}\Hash
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Updates\NionjZ\Id
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Updates\NionjZ\Index
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{8ECD3971-5904-4747-A164-F005E421259E}\Triggers
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{8ECD3971-5904-4747-A164-F005E421259E}\DynamicInfo
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ConfigValueEssNeedsLoading
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\List of event-active namespaces
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v4.0.30319_32\Start
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 NT\CurrentVersion\SoftwareProtectionPlatform\ServiceSessionId

Network Behavior



Name	IP	Country	ASN	ASN Name	Trigger Process Type

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.09233307838	Sandbox	224.0.0.252	5355
3.09350609779	Sandbox	224.0.0.252	5355
3.11321806908	Sandbox	239.255.255.250	3702
3.12963795662	Sandbox	192.168.56.255	137
5.6468091011	Sandbox	224.0.0.252	5355
9.12898492813	Sandbox	192.168.56.255	138

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\TmpF03C.Tmp	Type : XML document text MD5 : 9ab430601bc0c4c7479a951663434f91 SHA-1 : 4883eebb8041de79fd4f20ae91519ae70d212383 SHA-256 : f81a5a864135bf16f18cff837f15ab09a0e6b9f50c38c25 SHA-512 : 55e76efed135f34699c0de5a34924cace3bfa3f6e655b3 Size : 1.556 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	29c8d201060f864bd41f4c57c767241e2f57ea9b
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1:	29c8d201060f864bd41f4c57c767241e2f57ea9b
MD5:	e00521e507bc8e874d98c2218423180a
First Seen Date:	2023-07-03 07:08:28.543170 (a day ago)
Number Of Clients Seen:	3
Last Analysis Date:	2023-07-03 10:29:27.464221 (about 24 hours ago)
Human Expert Analysis Date:	2023-07-04 09:46:08.658889 (41 minutes ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

 PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[{"u'Path': u'gPUB.pdb\x00', "u'GUID': u'{4430e675-0bbd-4490-a7e1-0b22f7ed332d}', "u'timestamp': u'2097-07-11 13:41:27'}]
Number Of Sections	3
Trid	[[56.7, u'Generic CIL Executable (.NET, Mono, etc.)], [21.3, u'Win64 Executable (generic)'], [10.1, u'Windows screen saver'], [5.0, u'Win32 Dynamic Link Library (generic)'], [3.4, u'Win32 Executable (generic)']]
Compilation Time Stamp	0xC74A799C [Sat Dec 14 10:59:40 2075 UTC] [SUSPICIOUS]
Translation	0x0000 0x04b0
LegalCopyright	Copyright \xa9 2019
Assembly Version	1.0.0.0
InternalName	gPUB.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	CRM02
ProductVersion	1.0.0.0
FileDescription	CRM02
OriginalFilename	gPUB.exe
Entry Point	0x4aeb9a (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	710144
Ssdeep	12288:bcj6mVPWC/5weFFqWWiKsKVQojUBwK1fAKRsD94cgE0G:fVOo5yWWi4QGEHRsDuEZ
Sha256	b5ed2d16101b333863529e10f2413b70ea33ffdafb65ec74ea849f9d425fdf91
Exifinfo	[{"u'EXE:FileSubtype': 0, "u'File:FilePermissions': 'rw-r--r-', "u'SourceFile': 'u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/2/9/c/8/29c8d201060f864bd41f4c57c767241e2f57ea9b', "u'EXE:OriginalFileName': 'u'gPUB.exe', "u'EXE:ProductName': 'u'CRM02', "u'EXE:InternalName': 'u'gPUB.exe', "u'File:MIMEType': 'u'application/octet-stream', "u'File:FileAccessDate': 'u'2023:07:03 07:08:17+00:00', "u'EXE:InitializedDataSize': 2048, "u'File:FileModifyDate': 'u'2023:06:30 18:00:34+00:00', "u'EXE:AssemblyVersion': 'u'1.0.0.0', "u'EXE:FileVersionNumber': 'u'1.0.0.0', "u'EXE:FileVersion': 'u'1.0.0.0', "u'File:FileSize': 'u'694 kB', "u'EXE:CharacterSet': 'u'Unicode', "u'EXE:MachineType': 'u'Intel 386 or later, and compatibles', "u'EXE:FileType': 'u'Win32', "u'EXE:LegalTrademarks': 'u'', "u'EXE:ProductVersion': 'u'1.0.0.0', "u'EXE:ObjectFileType': 'u'Executable application', "u'File:FileType': 'u'Win32 EXE', "u'EXE:CompanyName': 'u'', "u'File:FileName': 'u'29c8d201060f864bd41f4c57c767241e2f57ea9b', "u'EXE:ImageVersion': 0.0, "u'File:FileTypeExtension': 'u'exe', "u'EXE:OSVersion': 4.0, "u'EXE:PEType': 'u'PE32', "u'EXE:TimeStamp': 'u'2075:12:14 10:59:40+00:00', "u'EXE:FileFlagsMask': 'u'0x003f', "u'EXE:LegalCopyright': 'u'Copyright \xa9 2019', "u'EXE:LinkerVersion': 48.0, "u'EXE:FileFlags': 'u'(none)', "u'EXE:Subsystem': 'u'Windows GUI', "u'File:Directory': 'u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/2/9/c/8', "u'EXE:FileDescription': 'u'CRM02', "u'EXE:EntryPoint': 'u'0xaeb9a', "u'EXE:SubsystemVersion': 4.0, "u'EXE:CodeSize': 707584, "u'EXE:Comments': 'u'', "u'File:FileinodeChangeDate': 'u'2023:06:30 18:00:35+00:00', "u'EXE:UninitializedDataSize': 0, "u'EXE:LanguageCode': 'u'Neutral', "u'ExifTool:ExifToolVersion': 10.1, "u'EXE:ProductVersionNumber': 'u'1.0.0.0'}]
Mime Type	application/x-dosexec
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x2000	0xacba0	0xacc00	7.39133126007	7282e129bbc5bded45e1d14e2b431f97
.rsrc	0xb0000	0x58c	0x600	4.0505846264	67885392154967f5d450a48b8f04e255
.reloc	0xb2000	0xc	0x200	0.101910425663	f1c572b87fc1639365ecbb93f18efec4

PE Imports

- mscoree.dll
 - _CorExeMain

PE Resources

```
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 721040, u'sha256': u'b0df994266bc548658af30af0068edb50d2250defce6a3ae2ee7777d69ec6f1', u'type': u'data', u'size': 764}  
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 721820, u'sha256': u'539dc26a14b6277e87348594ab7d6e932d16aabb18612d77f29fe421a9f1d46a', u'type': u'XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators', u'size': 490}
```

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS

