VALKYRIE COMODO

Summary

File Name: 9ea7d8ba25a4bad3016c138b414c5613d1b9df79

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

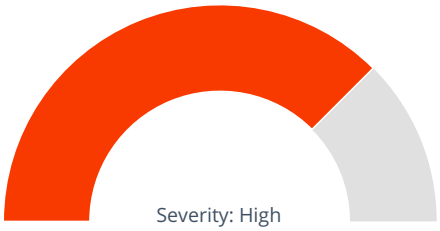
SHA1: 9ea7d8ba25a4bad3016c138b414c5613d1b9df79

MD5: 5b1a0d21643c69a853ebdad223d6bbc0

MALWARE

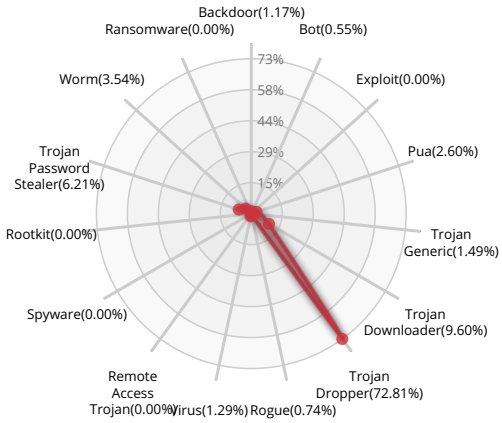
Valkyrie Final Verdict

DETECTION SECTION

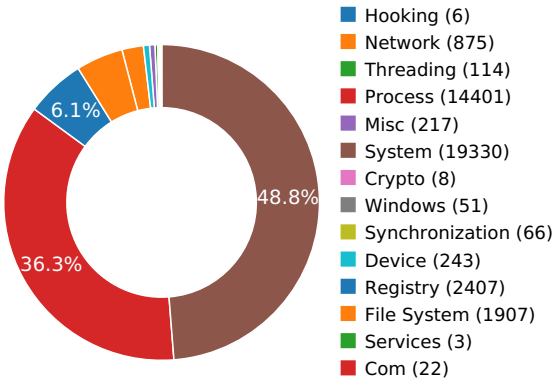


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

NETWORKING

Attempts to connect to a dead IP:Port (3 unique times) — Show sources

Performs some HTTP requests — Show sources

MALWARE ANALYSIS SYSTEM EVASION

Detects VMware through the presence of a registry key — Show sources

Checks the presence of disk drives in the registry, possibly for anti-virtualization — Show sources

Attempts to identify installed analysis tools by registry key — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

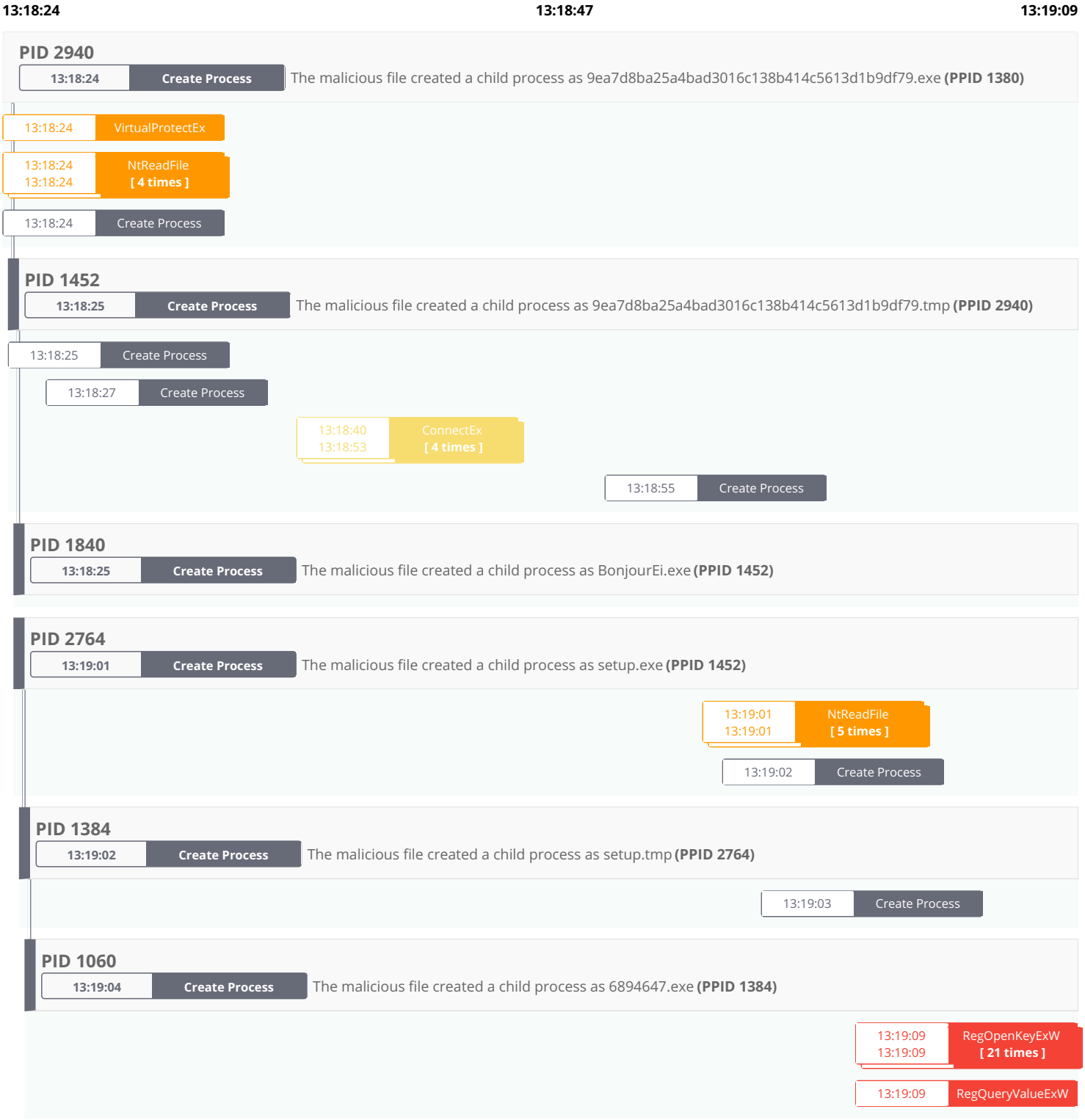
Creates RWX memory — Show sources

DATA OBFUSCATION

Drops a binary and executes it — Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Users\user\AppData\Local\Temp\netmsg.dll
C:\Windows\System32\netmsg.dll
C:\Users\user\AppData\Local\Temp\9ea7d8ba25a4bad3016c138b414c5613d1b9df79.exe
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\is-B1JA9.tmp
C:\Users\user\AppData\Local\Temp\is-B1JA9.tmp\9ea7d8ba25a4bad3016c138b414c5613d1b9df79.tmp
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Fonts\staticcache.dat
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\is-B1JA9.tmp\netmsg.dll
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp_isetup
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\idp.dll
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\itdownload.dll
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\itdownload.ENU
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\itdownload.ENU.DLL
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\itdownload.EN
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\itdownload.EN.DLL
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\setup.exe.config
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\BonjourEi.exe.config
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\BonjourEi.exe
C:\ProgramData\Microsoft\Network\Connections\Pbk\rasphone.pbk
C:\ProgramData\Microsoft\Network\Connections\Pbk*.pbk
C:\Windows\System32\ras*.pbk
C:\Users\user\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk
C:\Users\user\AppData\Roaming\Microsoft\Network\Connections\Pbk*.pbk
C:\Windows\System32\en-US\WINHTTP.dll.mui
C:\Users\user\AppData\LocalLow
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6BADA8974A10C4BD62CC921D13E43B18_EE9DB89C3D6A328B5FEAFF0ED3C77874
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_EE9DB89C3D6A328B5FEAFF0ED3C77874
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\1E698CCB2C296D265AC1A253974E09FD_A2E7FF7CFBC6B9BF06CE29B23F0D7A5A
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\1E698CCB2C296D265AC1A253974E09FD_A2E7FF7CFBC6B9BF06CE29B23F0D7A5A
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\D57B3BFF6E0B79FBD8CB6482C7775D35
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C07822D66105396A1B8E01486E66C5F3
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\D57B3BFF6E0B79FBD8CB6482C7775D35
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\C07822D66105396A1B8E01486E66C5F3
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\setup.exe
C:\Windows\sysnative\MSCOREE.DLL.local
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework64*
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\clr.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\sysnative\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\system\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\ProgramData\Oracle\Java\javapath\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\sysnative\wbem\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\sysnative\WindowsPowerShell\v1.0\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Universal Extractor\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Python27\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Python27\Scripts\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\sysinternals\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\IDA_Pro_v6\python\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\BonjourEi.exe.Local\
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6

C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\msvcr80.dll
C:\Windows
C:\Windows\winsxs
C:\Windows\Microsoft.NET\Framework64\v4.0.30319
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\fusion.localgac
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\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\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\453CB2B5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoProxyDetectType
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\9ea7d8ba25a4bad3016c138b414c5613d1b9df79_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\9ea7d8ba25a4bad3016c138b414c5613d1b9df79_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\9ea7d8ba25a4bad3016c138b414c5613d1b9df79_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\9ea7d8ba25a4bad3016c138b414c5613d1b9df79_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\9ea7d8ba25a4bad3016c138b414c5613d1b9df79_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\9ea7d8ba25a4bad3016c138b414c5613d1b9df79_RASAPI32\FileDirectory
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\9ea7d8ba25a4bad3016c138b414c5613d1b9df79_RASMANCS\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\9ea7d8ba25a4bad3016c138b414c5613d1b9df79_RASMANCS\FileTracingMask

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\9ea7d8ba25a4bad3016c138b414c5613d1b9df79_RASMANCS\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\9ea7d8ba25a4bad3016c138b414c5613d1b9df79_RASMANCS\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\9ea7d8ba25a4bad3016c138b414c5613d1b9df79_RASMANCS\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\9ea7d8ba25a4bad3016c138b414c5613d1b9df79_RASMANCS\FileDirectory
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ProgramData
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\WinHttpSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Local AppData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\EnableInetUnknownAuth
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\CLRLoadLogDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\OnlyUseLatestCLR

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\is-B1JA9.tmp\9ea7d8ba25a4bad3016c138b414c5613d1b9df79.tmp
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\idp.dll
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\itdownload.dll
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\setup.exe.config
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\BonjourEi.exe.config
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\BonjourEi.exe
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6BADA8974A10C4BD62CC921D13E43B18_EE9DB89C3D6A328B5FEAFF0ED3C77874
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_EE9DB89C3D6A328B5FEAFF0ED3C77874
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\1E698CCB2C296D265AC1A253974E09FD_A2E7FF7CFBC6B9BF06CE29B23F0D7A5A
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\1E698CCB2C296D265AC1A253974E09FD_A2E7FF7CFBC6B9BF06CE29B23F0D7A5A
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\D57B3BFF6E0B79FBD8CB6482C7775D35
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\D57B3BFF6E0B79FBD8CB6482C7775D35

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C07822D66105396A1B8E01486E66C5F3

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\C07822D66105396A1B8E01486E66C5F3

C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\setup.exe

C:\Windows\sysnative\drivers\etc\hosts

C:\Users\user\AppData\Local\Google\Chromee\User Data\Default\Preferences

C:\Users\user\AppData\Local\Temp\is-1A7UH.tmp\setup.tmp

C:\Users\user\AppData\Local\Temp\is-VQ6UB.tmp_isetup_setup64.tmp

C:\Users\user\AppData\Local\Temp\is-VQ6UB.tmp\DRDRE.exe

C:\Users\user\AppData\Local\Temp\is-VQ6UB.tmp\is-3J3M5.tmp

C:\Users\user\AppData\Local\Temp\is-VQ6UB.tmp\DRDRE.exe.config

C:\Users\user\AppData\Local\Temp\is-VQ6UB.tmp\is-GUBFE.tmp

C:\Program Files (x86)\trs\6894647.exe

C:\Program Files (x86)\trs\6894647.exe.config

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

C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch.1060.24896078

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

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

C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.1060.24896078

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

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

C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.1060.24896078

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

RESOLVED APIS

kernel32.dll.SetDllDirectoryW

kernel32.dll.SetSearchPathMode

kernel32.dll.SetProcessDEPPolicy

kernel32.dll.Wow64DisableWow64FsRedirection

kernel32.dll.Wow64RevertWow64FsRedirection

kernel32.dll.GetUserDefaultUILanguage

comctl32.dll.RegisterClassNameW

kernel32.dll.SortGetHandle

kernel32.dll.SortCloseHandle

uxtheme.dll.ThemeInitApiHook

user32.dll.IsProcessDPIAware

dwmapi.dll.DwmIsCompositionEnabled
uxtheme.dll.EnableThemeDialogTexture
advapi32.dll.UnregisterTraceGuids
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
gdi32.dll.GetTextFaceAliasW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
gdi32.dll.GetFontAssocStatus
advapi32.dll.RegQueryValueExA
advapi32.dll.RegEnumKeyExW
gdi32.dll.GdiIsMetaPrintDC
ole32.dll.CoInitializeEx
ole32.dll.CoUninitialize
cryptbase.dll.SystemFunction036
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoRevokeInitializeSpy
uxtheme.dll.OpenThemeData
uxtheme.dll.CloseThemeData
uxtheme.dll.DrawThemeBackground
uxtheme.dll.DrawThemeText
uxtheme.dll.GetThemeBackgroundContentRect
uxtheme.dll.GetThemePartSize
uxtheme.dll.GetThemeTextExtent
uxtheme.dll.GetThemeTextMetrics
uxtheme.dll.GetThemeBackgroundRegion
uxtheme.dll.HitTestThemeBackground
uxtheme.dll.DrawThemeEdge
uxtheme.dll.DrawThemeIcon
uxtheme.dll.IsThemePartDefined
uxtheme.dll.IsThemeBackgroundPartiallyTransparent

uxtheme.dll.GetThemeColor
uxtheme.dll.GetThemeMetric
uxtheme.dll.GetThemeString
uxtheme.dll.GetThemeBool
uxtheme.dll.GetThemeInt
uxtheme.dll.GetThemeEnumValue
uxtheme.dll.GetThemePosition
uxtheme.dll.GetThemeFont
uxtheme.dll.GetThemeRect
uxtheme.dll.GetThemeMargins
uxtheme.dll.GetThemeIntList
uxtheme.dll.GetThemePropertyOrigin
uxtheme.dll.SetWindowTheme
uxtheme.dll.GetThemeFilename
uxtheme.dll.GetThemeSysColor
uxtheme.dll.GetThemeSysColorBrush
uxtheme.dll.GetThemeSysBool
uxtheme.dll.GetThemeSysSize
uxtheme.dll.GetThemeSysFont
uxtheme.dll.GetThemeSysString
uxtheme.dll.GetThemeSysInt
uxtheme.dll.IsThemeActive
uxtheme.dll.IsAppThemed
uxtheme.dll.GetWindowTheme
uxtheme.dll.IsThemeDialogTextureEnabled
uxtheme.dll.GetThemeAppProperties
uxtheme.dll.SetThemeAppProperties
uxtheme.dll.GetCurrentThemeName
uxtheme.dll.GetThemeDocumentationProperty
uxtheme.dll.DrawThemeParentBackground

DELETED FILES

C:\Users\user\AppData\Local\Temp\is-B1JA9.tmp\9ea7d8ba25a4bad3016c138b414c5613d1b9df79.tmp
C:\Users\user\AppData\Local\Temp\is-B1JA9.tmp
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\BonjourEi.exe

C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\BonjourEi.exe.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch.1840.24863218
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.1840.24863218
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.1840.24863265
C:\Users\user\AppData\Local\Temp\is-1A7UH.tmp\setup.tmp
C:\Users\user\AppData\Local\Temp\is-1A7UH.tmp
C:\Users\user\AppData\Local\Temp\is-VQ6UB.tmp\is-3J3M5.tmp
C:\Users\user\AppData\Local\Temp\is-VQ6UB.tmp\is-GUBFE.tmp
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch.1060.24896078
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch.new
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.1060.24896078
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.new
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.1060.24896078
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.new

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
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
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\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\9ea7d8ba25a4bad3016c138b414c5613d1b9df79.tmp
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization
HKEY_LOCAL_MACHINE\Software\Microsoft\SQMClient\Windows\DisabledProcesses\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\453CB2B5
HKEY_LOCAL_MACHINE\Software\Microsoft\SQMClient\Windows\DisabledSessions\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner

HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
HKEY_CURRENT_USER\Software\Borland\Locales
HKEY_LOCAL_MACHINE\Software\Borland\Locales
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales
HKEY_CURRENT_USER\Software\Classes
HKEY_CURRENT_USER\Software\Classes\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\TreatAs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\Progid

EXECUTED COMMANDS

"C:\Users\user\AppData\Local\Temp\is-B1JA9.tmp\9ea7d8ba25a4bad3016c138b414c5613d1b9df79.tmp" /SL5="$1501DC,321605,136192,C:\Users\user\AppData\Local\Temp\9ea7d8ba25a4bad3016c138b414c5613d1b9df79.exe"
"C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\BonjourEi.exe"
"C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\setup.exe"
"C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\setup.exe" /VERYSILENT /m=5 /id=305a2a5da2db16e3.16940204
"C:\Users\user\AppData\Local\Temp\is-1A7UH.tmp\setup.tmp" /SL5="$10017E,430318,57856,C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\setup.exe" /VERYSILENT /m=5 /id=305a2a5da2db16e3.16940204
"C:\Program Files (x86)\trs\6894647.exe" 5 305a2a5da2db16e3.16940204 0 0 0

READ FILES

C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Windows\System32\netmsg.dll
C:\Users\user\AppData\Local\Temp\9ea7d8ba25a4bad3016c138b414c5613d1b9df79.exe
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Fonts\staticcache.dat
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\idp.dll
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\itdownload.dll
C:\Windows\System32\en-US\WINHTTP.dll.mui
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6BADA8974A10C4BD62CC921D13E43B18_EE9DB89C3D6A328B5FEAFF0ED3C77874
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_EE9DB89C3D6A328B5FEAFF0ED3C77874
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\1E698CCB2C296D265AC1A253974E09FD_A2E7FF7CFBC6B9BF06CE29B23F0D7A5A
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\1E698CCB2C296D265AC1A253974E09FD_A2E7FF7CFBC6B9BF06CE29B23F0D7A5A
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\D57B3BFF6E0B79FBD8CB6482C7775D35
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C07822D66105396A1B8E01486E66C5F3
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\D57B3BFF6E0B79FBD8CB6482C7775D35
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\C07822D66105396A1B8E01486E66C5F3
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\BonjourEi.exe.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\msvcr80.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_64\index142.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\9469491f37d9c35b596968b206615309\mscorlib.ni.dll
C:\Windows\sysnative\l_intl.nls

C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\BonjourEi.exe
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\BonjourEi.exe.Config
C:\Windows\assembly\NativeImages_v2.0.50727_64\System\adff7dd9fe8e541775c46b6363401b22\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\5910828a337dbe848dc90c7ae0a7dee2\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Windows.Forms\6c352ff9e3603b0e69d969ff7e7632f5\System.Windows.Forms.ni.dll
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Culture.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorrc.dll
C:\Windows\sysnative\drivers\etc\hosts
C:\Users\user\AppData\Local\Temp\is-4B3OL.tmp\setup.exe
C:\Users\user\AppData\Local\Temp\is-VQ6UB.tmp_isetup_setup64.tmp
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Windows\System32\imageres.dll
C:\Windows\System32\shell32.dll
C:\
C:\Users\user\AppData\Local\Temp\is-VQ6UB.tmp\DRDRE.exe
C:\Windows\winsxs\FileMaps\users_user_appdata_local_temp_is-vq6ub.tmp_9b1a90e5ea340ed5.cdf-ms
C:\Users\user\AppData\Local\Temp\is-VQ6UB.tmp\is-3J3M5.tmp
C:\Users\user\AppData\Local\Temp\is-VQ6UB.tmp\is-GUBFE.tmp
C:\Users\user\AppData\Local\Temp\is-VQ6UB.tmp\DRDRE.exe.config
C:\Program Files (x86)\trs\6894647.exe.config
C:\Program Files (x86)\trs\6894647.exe
C:\Program Files (x86)\trs\6894647.exe.Config
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Configuration\091b931d0f6408001747dbbbb05dbe66\System.Configuration.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Xml\ee795155543768ea67eecddc686a1e9e\System.Xml.ni.dll
C:\Windows\sysnative\tzres.dll

MUTEXES

CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511

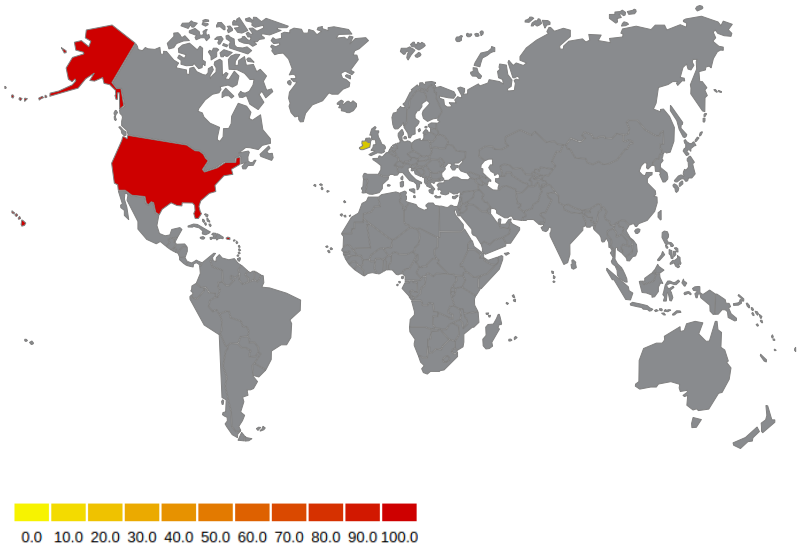
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000
IESQMMUTEX_0_208
Global\CLR_CASOFF_MUTEX
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0001
DefaultTabtip-MainUI
Global\.net clr networking

MODIFIED REGISTRY KEYS

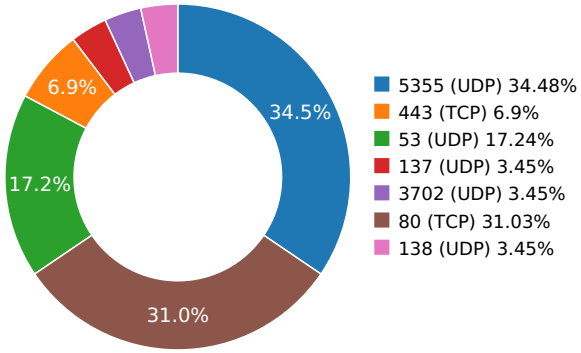
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0001
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0001\Owner
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0001\SessionHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0001\Sequence
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0001\RegFiles0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0001\RegFilesHash

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	23.215.130.203	United States	20940	Akamai Technologies, Inc.	OS Process
	52.218.52.154	Ireland	16509	Amazon Technologies Inc.	Malware Process
ctldl.windowsupdate.com	63.238.216.8	United States	209	Qwest Communications Com..	OS Process
crl4.digicert.com	66.225.197.197	United States	30081	Server Central Network	Malware Process
crl3.digicert.com	72.21.91.29	United States	15133	MCI Communications Servic...	Malware Process
ocsp.digicert.com	72.21.91.29	United States	15133	MCI Communications Servic...	Malware Process
s3-eu-west-1.amazonaws.com	52.218.52.44	Ireland	16509	Amazon Technologies Inc.	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	21.0993249416
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?65c5493cec8ec257 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?65c5493cec8ec257						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	27.6102149487
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEAGC%2BAmOouYmuRo7J4Qfua8%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEAGC%2BAmOouYmuRo7J4Qfua8%3D						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	33.9702329636
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTuqL92L3tjkN67RNFF%2FEdvT6NEzAQUwBKyKHRoRmfpcCV0GgBFWwZ9XEQCEA7cK%2FJk9VZxucRii0Q9yCY%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTuqL92L3tjkN67RNFF%2FEdvT6NEzAQUwBKyKHRoRmfpcCV0GgBFWwZ9XEQCEA7cK%2FJk9VZxucRii0Q9yCY%3D						
crl3.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	34.4035670757
Path: /DigiCertBaltimoreCA-2G2.crl **URI:** http://crl3.digicert.com/DigiCertBaltimoreCA-2G2.crl						
crl4.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	34.4569809437
Path: /DigiCertBaltimoreCA-2G2.crl **URI:** http://crl4.digicert.com/DigiCertBaltimoreCA-2G2.crl						

DNS QUERIES

Request	Type
s3-eu-west-1.amazonaws.com	A
Answers - 52.218.52.154 (A)	
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 23.215.130.195 (A) - a1621.g.akamai.net (CNAME) - ctldl.windowsupdate.com.edgesuite.net (CNAME) - 23.215.130.203 (A)	
ocsp.digicert.com	A
Answers - cs9.wac.phicdn.net (CNAME) - 72.21.91.29 (A)	
crl3.digicert.com	A
crl4.digicert.com	A
Answers - digicert.cachefly.net (CNAME) - 66.225.197.197 (A) - rvip1.ue.cachefly.net (CNAME)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
12.7196469307	Sandbox	52.218.52.154	443
21.0993249416	Sandbox	23.215.130.203	80
27.6102149487	Sandbox	72.21.91.29	80
34.2285599709	Sandbox	52.218.52.154	443
34.4035670757	Sandbox	72.21.91.29	80
34.4569809437	Sandbox	66.225.197.197	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.06670308113	Sandbox	224.0.0.252	5355
3.0874080658	Sandbox	224.0.0.252	5355
3.09290909767	Sandbox	239.255.255.250	3702
3.1280310154	Sandbox	192.168.56.255	137
5.64674401283	Sandbox	224.0.0.252	5355
6.14324498177	Sandbox	192.168.56.255	138
9.73594307899	Sandbox	224.0.0.252	5355
12.5801029205	Sandbox	8.8.4.4	53
15.3915688992	Sandbox	224.0.0.252	5355
18.2519989014	Sandbox	224.0.0.252	5355
21.0172488689	Sandbox	8.8.4.4	53
21.9707429409	Sandbox	224.0.0.252	5355
24.8315870762	Sandbox	224.0.0.252	5355
27.5660190582	Sandbox	8.8.4.4	53
28.4390189648	Sandbox	224.0.0.252	5355
31.3295559883	Sandbox	224.0.0.252	5355
34.3144218922	Sandbox	8.8.4.4	53
34.3921279907	Sandbox	8.8.4.4	53

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Is-B1JA9.Tmp\9ea7d8ba25a4bad3016c138b414c5613d1b9df79.Tmp	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 99a2c64db21979483ac66bba0883978b **SHA-1 :** be654b319dd9d9759c0366126db46d95218ed1ac **SHA-256 :** 2f9347250bb61c8026d8460ccc8f5e103d603058 **SHA-512 :** 583fb26bb5e6f997a3ac0dfdc2d8b1416989cab9 **Size :** 792.064 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-4B3OL.Tmp\Idp.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** b37377d34c8262a90ff95a9a92b65ed8 **SHA-1 :** faeef415bd0bc2a08cf9fe1e987007bf28e7218d **SHA-256 :** e5a0ad2e37dde043a0dd4ad7634961ff3f0d70e8 **SHA-512 :** 69d8da5b45d9b4b996d32328d3402fa37a3d710 **Size :** 221.184 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\1E698CCB2C296D265AC1A253974E09FD_A2E7FF7CFBC6B9BF06CE29B23F0D7A5A	**Type :** data **MD5 :** 149b2ff950fc9d13073323594b217d57 **SHA-1 :** d43ece70d21a2ce7e9c62363bb76b920dfc3c426 **SHA-256 :** 6859fc345ec7c954881e2b69c61864019f7597aa4 **SHA-512 :** 2203e664e3e448ae57e23d8e636604fa6848b11b **Size :** 0.434 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\1E698CCB2C296D265AC1A253974E09FD_A2E7FF7CFBC6B9BF06CE29B23F0D7A5A	**Type :** data **MD5 :** dd9d1264a431cd97b8fe60efbed079ac **SHA-1 :** dbf144490cbb25f5bcc3606709920ecb1d094397 **SHA-256 :** 34f1fc1ec3bd4479e7909608bb7c8069620bf09b **SHA-512 :** e0b2162215fa403e0582aae3a9c99d54aefb2ce1 **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-VQ6UB.Tmp\DRDRE.Exe.Config **C:\Program Files (X86)\Trs\6894647.Exe.Config**	**Type :** XML document text **MD5 :** deb1b377008e7c7a9bc805b740245d6b **SHA-1 :** 0fdb500ae344c4271a97c96c100a8ce1795abf3b **SHA-256 :** 54ef8c6bf905be93b7d4c031d7f26ac62f324f7d3 **SHA-512 :** 03f744551109ebd908dfe7f2a6755049e6b87089 **Size :** 1.86 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** Microsoft Cabinet archive data, 6509 bytes, 1 file **MD5 :** 33b39e2a516ef730a8fa922894f0fbd5 **SHA-1 :** 03d455583dda59215d945af76af6293b202f586f **SHA-256 :** 9446e8f2056fea3ac1365a809ada04602606242c **SHA-512 :** 75763aa13b43eb96294b0f84e13106611198872 **Size :** 6.509 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\D57B3BFF6E0B79FBD8CB6482C7775D35	**Type :** data **MD5 :** 1231ef327e3fb8d6a93bc964906af3e5 **SHA-1 :** 84f7071e434c0818489cc724703878385cf12460 **SHA-256 :** 83f0f8df4661a607a7a4ec80d5e885de35f889719 **SHA-512 :** 44c1e904a1a2a398b44a75fe2e8fb1812d3ed411 **Size :** 0.248 Kilobytes.
C:\Windows\Sysnative\Drivers\Etc\Hosts	**Type :** ASCII text, with CRLF line terminators **MD5 :** dcda9146bd9250cc91168c3f77306a2e **SHA-1 :** af494df3d1bad30488d5bf3d2fb5b63489d68eb3 **SHA-256 :** 838dc012916563896951a35577d0101ea5145d3 **SHA-512 :** 078e7e10ec90d7dfd6232f7033582f7ed76b8633 **Size :** 1.399 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Is-1A7UH.Tmp\Setup.Tmp	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 832dab307e54aa08f4b6cdd9b9720361 **SHA-1 :** ebd007fb7482040ecf34339e4bf917209c1018df **SHA-256 :** cc783a04ccbca4edd06564f8ec88fe5a15f1e3bb2 **SHA-512 :** 358d43522fd460eb1511708e4df22ea454a95e5b **Size :** 713.728 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-4B3OL.Tmp_isetup_setup64.Tmp **C:\Users\User\AppData\Local\Temp\Is-VQ6UB.Tmp_isetup_setup64.Tmp**	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** e4211d6d009757c078a9fac7ff4f03d4 **SHA-1 :** 019cd56ba687d39d12d4b13991c9a42ea6ba03da **SHA-256 :** 388a796580234efc95f3b1c70ad4cb44bfddc7ba **SHA-512 :** 17257f15d843e88bb78adcfb48184b8ce22109cc **Size :** 6.144 Kilobytes.
C:\Windows\Microsoft.NET\Framework64\V2.0.50727\CONFIG\Security.Config.Cch **C:\Users\User\AppData\Roaming\Microsoft\CLR Security Config\V2.0.50727.312\64bit\Security.Config.Cch** **C:\Windows\Microsoft.NET\Framework64\V2.0.50727\CONFIG\Enterprisesec.Config.Cch**	**Type :** data **MD5 :** 21c8a7044feda44334c6f25cbe2c917b **SHA-1 :** a08c94aad2962168bf54ccbcd7801daf3575852d **SHA-256 :** 1ec19ae1d03c03015cedb095baf67192356cf5e8 **SHA-512 :** b15858f78599a8f992eebe056457d6002984d241 **Size :** 1.212 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C07822D66105396A1B8E01486E66C5F3	**Type :** data **MD5 :** ae776cc08c6bfe4e05f3e9dcb6c2b5fd **SHA-1 :** f8502e01d429f7a16707ad68de91979c0feba6ae **SHA-256 :** e86aecfea259be2acbef5bda8b7f87a45ba9e602f **SHA-512 :** e709c5ffd1413c50ec2129f5e4c76d9e0ac2d5463 **Size :** 0.222 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-4B3OL.Tmp\Setup.Exe.Config	**Type :** XML document text **MD5 :** 85ff7012c2e71989252d52213bb9ab5d **SHA-1 :** e52d18847fe27ad9c8b5554de28251cf53b6db21 **SHA-256 :** c21bc30ca71308946b5a0bfaf4435dcea3d47d1b **SHA-512 :** ba5c5efe43a4300800c74e9e828a796e716b5e2b **Size :** 1.862 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** eb05e12f3dbe0834ed6c903752b7f6a3 **SHA-1 :** 43441b64f85dc2616f40cdbaa7e2d8e2015d1851 **SHA-256 :** b9e0698e7288c4d802a465b879a7287d6e483f5e **SHA-512 :** 42429693aa2760dbe0475a52db3441ca0cd90b1 **Size :** 0.342 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-VQ6UB.Tmp\DRDRE.Exe **C:\Program Files (X86)\Trs\6894647.Exe**	**Type :** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** f2661647d6579b96159f9df4be9a0a54 **SHA-1 :** 9f7cbd1443d5bf7ea29de643fd4b1150c23403d8 **SHA-256 :** e09a4df7c00dc7d8058fdca67db2598634d41df1 **SHA-512 :** 4bf569eaeabc098b338160905d85449fba84383c **Size :** 670.208 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\C07822D66105396A1B8E01486E66C5F3 **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\D57B3BFF6E0B79FBD8CB6482C7775D35**	**Type :** data **MD5 :** c9fffae33637feb9275fcb554f1f44c7 **SHA-1 :** 5df728de2dbd208d7e3352b238dcedb10d46964a **SHA-256 :** a6822392d7234ebc2698bb1415aede4e27dd8c8 **SHA-512 :** 7b625aad45eff49f17851ccc15bcf5b376a08fd454 **Size :** 72.276 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Is-4B3OL.Tmp\BonjourEi.Exe.Config	**Type :** XML document text **MD5 :** 3f1498c07d8713fe5c315db15a2a2cf3 **SHA-1 :** ef5f42fd21f6e72bdc74794f2496884d9c40bbfb **SHA-256 :** 52ca39624f8fd70bc441d055712f115856bc67b3 **SHA-512 :** cb32ce5ef72548d1b0d27f3f254f4b67b23a0b66 **Size :** 1.86 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6BADA8974A10C4BD62CC921D13E43B18_EE9DB89C3D6A328B5FEAFF0ED3C77874	**Type :** data **MD5 :** 2c1d64f416e15ee9061961126c868c9b **SHA-1 :** 103262e82827ec57241be3402acb3cf6f5fba0b8 **SHA-256 :** 048865e5ba2d3635c8af2a74a74c2f9f14784b54 **SHA-512 :** ba1add04c1fb99c568f284106c39249aaa04ef2c4 **Size :** 0.438 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-4B3OL.Tmp\Setup.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 862dc00824907569471ebf85634d5ff9 **SHA-1 :** 354eff08c51bb21e4bbff602d7885f448a2599c0 **SHA-256 :** 323186c8a74461e33010c6a2b75a9cd2fafd265d **SHA-512 :** dfde0facb7b6c5a04a43a4ff990a1a16ebbf17f63 **Size :** 676.87 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-4B3OL.Tmp\BonjourEi.Exe	**Type :** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 3b3f9556fbd3dbb7986ae1ccf5ac41e4 **SHA-1 :** 557b649a76d9ea0a7f8dddca80b5b8ebee22bdc4 **SHA-256 :** 136699494da819541826d2d96548f7876a37647 **SHA-512 :** ee895e63f9bb0b7d62ce6caaf17c26ba22de49f0 **Size :** 19.968 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6BADA8974A10C4BD62CC921D13E43B18_EE9DB89C3D6A328B5FEAFF0ED3C77874	**Type :** data **MD5 :** 58053ece2ea6051309cab216d7de87be **SHA-1 :** 1728285384a90fb90f5071ee9e4cb7ca91387e5c **SHA-256 :** 69c5f8a8fb3f2299c289c37e11b454dafc66cb707 **SHA-512 :** 0c32db6977d41b08035b19e076982fbb491e28a **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-4B3OL.Tmp\Itdownload.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** d82a429efd885ca0f324dd92afb6b7b8 **SHA-1 :** 86bbdaa15e6fc5c7779ac69c84e53c43c9eb20ea **SHA-256 :** b258c4d7d2113dee2168ed7e35568c8e03341e2 **SHA-512 :** 5bf0c3b8fa5db63205a263c4fa5337188173248b **Size :** 205.312 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	9ea7d8ba25a4bad3016c138b414c5613d1b9df79
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	9ea7d8ba25a4bad3016c138b414c5613d1b9df79
MD5:	5b1a0d21643c69a853ebdad223d6bbc0
First Seen Date:	2018-05-23 10:02:41.207138 (7 months ago)
Number Of Clients Seen:	1
Last Analysis Date:	2018-05-23 10:02:41.207138 (7 months ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	8
Trid	[[81.5, u'Inno Setup installer'], [10.5, u'Win32 Executable Delphi generic'], [3.3, u'Win32 Executable (generic)'], [1.5, u'Win16/32 Executable Delphi generic'], [1.4, u'Generic Win/DOS Executable']]
Compilation Time Stamp	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC] [SUSPICIOUS]
LegalCopyright	
FileVersion	
CompanyName	
Comments	This installation was built with Inno Setup.
ProductName	Move
ProductVersion	9.6.8
FileDescription	Move Setup
Translation	0x0000 0x04b0
Entry Point	0x40aa98 (CODE)
Machine Type	Intel 386 or later - 32Bit
File Size	583077
Ssdeep	12288:77blM3BoO16DOpXz+4Bxmuc/braYNS72Lim:77blA31jpK4BMH6YAO
Sha256	a2ab46dfeb0ca42b5c648bc94c5005d7b7c9dc7fa2d44f50d4da11f7a949fefd
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/9/e/a/7/9ea7d8ba25a4bad3016c138b414c5613d1b9df79', u'EXE:ProductName': u'Move ', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:05:23 10:02:10+00:00', u'EXE:InitializedDataSize': 93696, u'File:FileModifyDate': u'2018:05:23 10:02:09+00:00', u'EXE:FileVersionNumber': u'0.0.0.0', u'EXE:FileVersion': u' ', u'File:FileSize': u'569 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': u'9.6.8 ', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u' ', u'File:FileName': u'9ea7d8ba25a4bad3016c138b414c5613d1b9df79', u'EXE:ImageVersion': 6.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 1.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'1992:06:19 22:22:17+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u' ', u'EXE:LinkerVersion': 2.25, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/9/e/a/7', u'EXE:FileDescription': u'Move Setup ', u'EXE:EntryPoint': u'0xaa98', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 41472, u'EXE:Comments': u'This installation was built with Inno Setup.', u'File:FileInodeChangeDate': u'2018:05:23 10:02:10+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'Neutral', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'0.0.0.0'}]
Mime Type	application/x-dosexec
Imphash	2fb819a19fe4dee5c03e8c6a79342f79

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0xa1d0	0xa200	6.64374902859	b7ea439d9c6d5ec722056c9243fb3054
DATA	0xc000	0x250	0x400	2.74012451302	9b2268ed5360951559d8041925d025fb
BSS	0xd000	0xe94	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0xe000	0x97c	0xa00	4.48607624623	df5f31e62e05c787fd29eed7071bf556
.tls	0xf000	0x8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0x10000	0x18	0x200	0.190488766435	14dfa4128117e7f94fe2f8d7dea374a0
.reloc	0x11000	0x91c	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x12000	0x15c5c	0x15e00	4.55397374136	c4ab1fc247159cd7fd9db7b3c58baa2e

PE Imports

- kernel32.dll
  - DeleteCriticalSection
  - LeaveCriticalSection
  - EnterCriticalSection
  - InitializeCriticalSection
  - VirtualFree
  - VirtualAlloc
  - LocalFree
  - LocalAlloc
  - WideCharToMultiByte
  - TlsSetValue
  - TlsGetValue
  - MultiByteToWideChar
  - GetModuleHandleA
  - GetLastError
  - GetCommandLineA
  - WriteFile
  - SetFilePointer
  - SetEndOfFile
  - RtlUnwind
  - ReadFile
  - RaiseException
  - GetStdHandle
  - GetFileSize
  - GetSystemTime
  - GetFileType
  - ExitProcess
  - CreateFileA
  - CloseHandle
- user32.dll
  - MessageBoxA
- oleaut32.dll
  - VariantChangeTypeEx
  - VariantCopyInd
  - VariantClear
  - SysStringLen
  - SysAllocStringLen
- advapi32.dll
  - RegQueryValueExA
  - RegOpenKeyExA
  - RegCloseKey
  - OpenProcessToken
  - LookupPrivilegeValueA
- kernel32.dll
  - WriteFile
  - VirtualQuery
  - VirtualProtect
  - VirtualFree
  - VirtualAlloc
  - Sleep
  - SizeofResource
  - SetLastError

    - SetFilePointer
    - SetErrorMode
    - SetEndOfFile
    - RemoveDirectoryA
    - ReadFile
    - LockResource
    - LoadResource
    - LoadLibraryA
    - IsDBCSLeadByte
    - GetWindowsDirectoryA
    - GetVersionExA
    - GetVersion
    - GetUserDefaultLangID
    - GetSystemInfo
    - GetSystemDirectoryA
    - GetSystemDefaultLCID
    - GetProcAddress
    - GetModuleHandleA
    - GetModuleFileNameA
    - GetLocaleInfoA
    - GetLastError
    - GetFullPathNameA
    - GetFileSize
    - GetFileAttributesA
    - GetExitCodeProcess
    - GetEnvironmentVariableA
    - GetCurrentProcess
    - GetCommandLineA
    - GetACP
    - InterlockedExchange
    - FormatMessageA
    - FindResourceA
    - DeleteFileA
    - CreateProcessA
    - CreateFileA
    - CreateDirectoryA
    - CloseHandle
- user32.dll
    - TranslateMessage
    - SetWindowLongA
    - PeekMessageA
    - MsgWaitForMultipleObjects
    - MessageBoxA
    - LoadStringA
    - ExitWindowsEx
    - DispatchMessageA
    - DestroyWindow
    - CreateWindowExA
    - CallWindowProcA
    - CharPrevA
- comctl32.dll
    - InitCommonControls
- advapi32.dll
    - AdjustTokenPrivileges

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 74580, u'sha256': u'54b2728de98f6355d30a067365a0dfdd86c34baddb5d4aedb79ad81bb08375f5', u'type': u'dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0', u'size': 9640}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 84220, u'sha256': u'5d47e9f3be453f075d500fc4d3b9d40cec41be4151a11366aa720948e7445267', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 85348, u'sha256': u'a4ddcad253a20b0f51ad1c580a56d7e943fd444d3417e19d1eba2748cb978928', u'type': u'dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0', u'size': 4264}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 89612, u'sha256': u'65e61d4a135007f40215bda147122d818d53dd7c3b4a32a39719f6e93710875d', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 67624}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 157236, u'sha256': u'2c0d32398e3c95657a577c044cc32fe24fa058d0c32e13099b26fd678de8354f', u'type': u'data', u'size': 754}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 157992, u'sha256': u'840989e0a92f2746ae60b8e3efc1a39bcca17e82df3634c1643d76141fc75bb3', u'type': u'data', u'size': 780}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 158772, u'sha256': u'26bda4da3649a575157a6466468a0a8694475664385595412 0fd715f3c9c7f78', u'type': u'data', u'size': 718}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 159492, u'sha256': u'd786490af7fe66042fb4a7d52023f5a1442f9b5e65d067b9093d1a128a6af34c', u'type': u'data', u'size': 104}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 159596, u'sha256': u'00a0794f0a493c167f64ed8b119d49bdc59f76bb35e5c295dc047095958ee2fd', u'type': u'data', u'size': 180}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 159776, u'sha256': u'34973a8a33b90ec734bd328198311f579666d5aeb04c94f469ebb822689de3c3', u'type': u'data', u'size': 174}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 159952, u'sha256': u'd6ed4ce193b2bf3f187138c156a233d36485f3baf7486bd351affb30cb56045b', u'type': u'data', u'size': 44}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 159996, u'sha256': u'76012ecb462f6375340bcf39935ccc054b7a4f6b9e433d0ea0a4fc0b66d55be9', u'type': u'MS Windows icon resource - 4 icons, 48x48', u'size': 62}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 160060, u'sha256': u'598775258c2ee00128d0b0d9716417121f04f6141a865a7b21236a0651251f7e', u'type': u'data', u'size': 1268}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 161328, u'sha256': u'356ca8abf11d97bf9dcbff47c04bf1ddcb8685ef84d38e6850ec6c28a37655b9', u'type': u'XML 1.0 document, ASCII text, with CRLF line terminators', u'size': 1580}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS