VALKYRIE COMODO

Summary

File Name: Trojan.MSIL.Crypt.dnbp-929b9dcfc8a43721ece5cb448cb486fbf5f5ded0f290eb1973a1ade67a1fab10

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

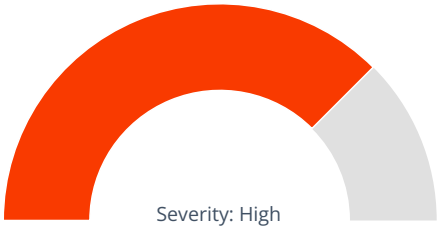
SHA1: c85530bfd84b61f2aaad539a348d3032b934f8a2

MD5: 630582ca84cc7d3b995c79cf19f67397

MALWARE

Valkyrie Final Verdict

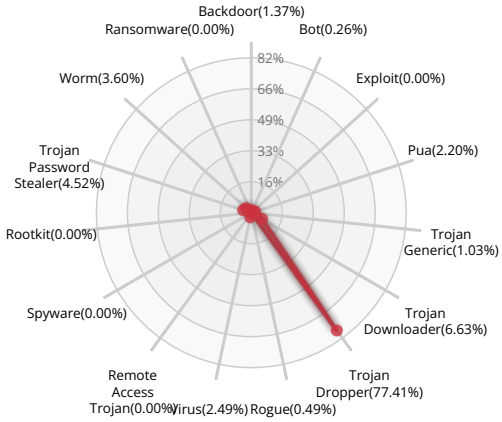
DETECTION SECTION



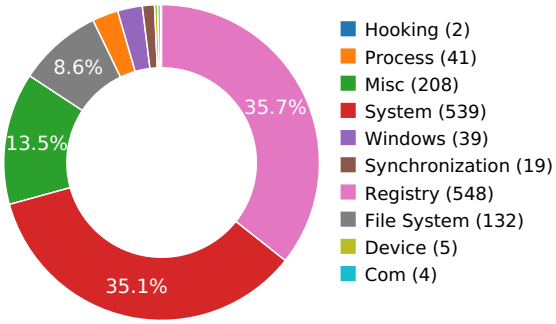
Severity: High

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

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

DATA OBFUSCATION

Drops a binary and executes it — Show sources

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\c85530bfd84b61f2aaad539a348d3032b934f8a2.exe
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\is-GE8VP.tmp
C:\Users\user\AppData\Local\Temp\is-GE8VP.tmp\c85530bfd84b61f2aaad539a348d3032b934f8a2.tmp
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Fonts\staticcache.dat
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\is-GE8VP.tmp\netmsg.dll
C:\Users\user\AppData\Local\Temp\is-F2R01.tmp
C:\Users\user\AppData\Local\Temp\is-F2R01.tmp_isetup
C:\Users\user\AppData\Local\Temp\is-F2R01.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-F2R01.tmp\isxdl.dll
C:\Windows\System32\msi.dll
C:\Users\user\AppData\Local\Temp\is-F2R01.tmp\dotnetchk.exe
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\is-GE8VP.tmp\c85530bfd84b61f2aaad539a348d3032b934f8a2.tmp.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
c:\directory
C:\Windows\System32\imageres.dll
C:\Windows\System32\shell32.dll
C:\Windows\win.ini
C:\Windows\System32\MSCOREE.DLL.local
C:\Windows\Microsoft.NET\Framework\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-F2R01.tmp\dotnetchk.exe.config

C:\Users\user\AppData\Local\Temp\is-F2R01.tmp\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

READ REGISTRY KEYS

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\4899F8E9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\AutoSuggest
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\Always Use Tab
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{03C036F1-A186-11D0-824A-00AA005B4383}\InProcServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{00BB2763-6A77-11D0-A535-00C04FD7D062}\InProcServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\Client\(Default)
HKEY_CURRENT_USER\Control Panel\Desktop\SmoothScroll
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\EnableBalloonTips
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewAlphaSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewShadow
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AccListViewV6
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\UseDoubleClickTimer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollInset
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\DragDelay
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\DragMinDist
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollDelay
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollInterval
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arabic Transparent

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arabic Transparent Bold

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arabic Transparent,0

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arabic Transparent Bold,0

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Helvetica

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arial Baltic,186

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arial CE,238

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arial CYR,204

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arial Greek,161

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arial TUR,162

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Courier New Baltic,186

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Courier New CE,238

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Courier New CYR,204

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Courier New Greek,161

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Courier New TUR,162

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Times

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Times New Roman Baltic,186

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Times New Roman CE,238

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Times New Roman CYR,204

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Times New Roman Greek,161

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Times New Roman TUR,162

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Tahoma Armenian

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Helv

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Tms Rmn

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\David Transparent

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\is-GE8VP.tmp\c85530bfd84b61f2aaad539a348d3032b934f8a2.tmp

C:\Users\user\AppData\Local\Temp\is-F2R01.tmp_isetup_setup64.tmp

C:\Users\user\AppData\Local\Temp\is-F2R01.tmp\isxdl.dll

C:\Users\user\AppData\Local\Temp\is-F2R01.tmp\dotnetchk.exe

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
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
uxtheme.dll.EnableTheming

REGISTRY KEYS

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\c85530bfd84b61f2aaad539a348d3032b934f8a2.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\4899F8E9
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\Internet Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Version
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\MS Sans Serif
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Tahoma
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Verdana
HKEY_LOCAL_MACHINE\Software\Policies
HKEY_CURRENT_USER\Software\Policies
HKEY_CURRENT_USER\Software
HKEY_LOCAL_MACHINE\Software

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\AutoSuggest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\Always Use Tab
HKEY_CLASSES_ROOT\CLSID\{03C036F1-A186-11D0-824A-00AA005B4383}\InProcServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{03C036F1-A186-11D0-824A-00AA005B4383}\InProcServer32\(Default)
HKEY_CLASSES_ROOT\CLSID\{00BB2763-6A77-11D0-A535-00C04FD7D062}\InProcServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{00BB2763-6A77-11D0-A535-00C04FD7D062}\InProcServer32\(Default)
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete\Client\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\Client\(Default)
HKEY_CURRENT_USER

EXECUTED COMMANDS

"C:\Users\user\AppData\Local\Temp\is-GE8VP.tmp\c85530bfd84b61f2aaad539a348d3032b934f8a2.tmp" /SL5="$60152,4397465,55808,C:\Users\user\AppData\Local\Temp\c85530bfd84b61f2aaad539a348d3032b934f8a2.exe"
"C:\Users\user\AppData\Local\Temp\is-F2R01.tmp\dotnetchk.exe"

READ FILES

C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Windows\System32\netmsg.dll
C:\Users\user\AppData\Local\Temp\c85530bfd84b61f2aaad539a348d3032b934f8a2.exe
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Fonts\staticcache.dat
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\is-F2R01.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-F2R01.tmp\isxdl.dll
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Windows\System32\imageres.dll
C:\Windows\System32\shell32.dll
C:\Windows\win.ini
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Users\user\AppData\Local\Temp\is-F2R01.tmp\dotnetchk.exe.config

MUTEXES

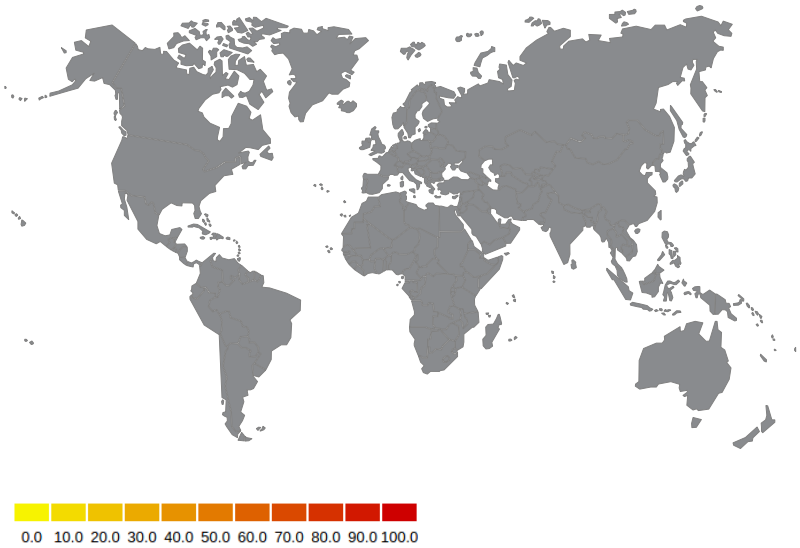
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000
DefaultTabtip-MainUI

MODIFIED REGISTRY KEYS

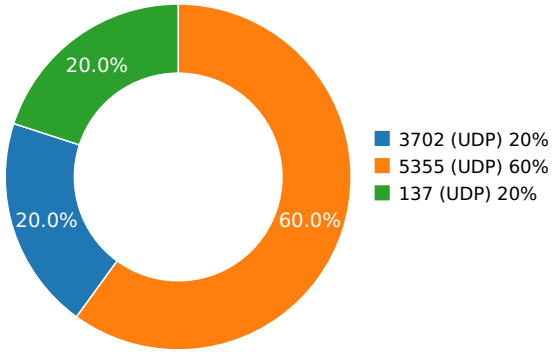
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
7.0863699913	Sandbox	224.0.0.252	5355
7.08691096306	Sandbox	224.0.0.252	5355
7.08773994446	Sandbox	239.255.255.250	3702
7.12491703033	Sandbox	192.168.56.255	137
9.63694906235	Sandbox	224.0.0.252	5355

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Is-F2R01.Tmp\Isxdl.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 792620390aae5305220283f2ce33ca68 **SHA-1 :** d9fee4cb3e2fa5e7d88b45662fd58b30aa9979f0 **SHA-256 :** 21bc620515ebbdeb125d273c2d8db45577d054(**SHA-512 :** 470914116f40e4f7216c840ccbc706eb7953c10e(**Size :** 59.392 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-F2R01.Tmp\Dotnetchk.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 26c5023438740dd0d532f33d6407919c **SHA-1 :** 2b38c639efa93eeb67fc47826c2be8ed8cef5cbb **SHA-256 :** e6ce9a0143c4c5aff4fab8199471230266b4b677 **SHA-512 :** 628f1b5ec369d842684ceab038ffabda33a1a2a4 **Size :** 61.632 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-GE8VP.Tmp\C85530bfd84b61f2aaad539a348d3032b934f8a2.Tmp	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** bb4bd737320b411d6c80203f0aaaa101 **SHA-1 :** cfa4893be9ddc75ff961e303b4852f4dd47b6145 **SHA-256 :** 2cdb61e71d0aee5d753c97813ce6f9ed5e4abacb **SHA-512 :** a032d79e5f31cf2fbd08e5b1e49598b8435d5b9b **Size :** 711.68 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-F2R01.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.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	Trojan.MSIL.Crypt.dnbp-929b9dcfc8a43721ece5cb448cb486fbf5f5ded0f290eb1973a1ade67a1fab10
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	c85530bfd84b61f2aaad539a348d3032b934f8a2
MD5:	630582ca84cc7d3b995c79cf19f67397
First Seen Date:	2023-07-26 19:36:44.507278 (about a year ago)
Number Of Clients Seen:	4
Last Analysis Date:	2023-07-26 20:45:10.873525 (about a year ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	8
Trid	[[77.7, u'Inno Setup installer'], [10.0, u'Win32 Executable Delphi generic'], [4.6, u'Win32 Dynamic Link Library (generic)'], [3.1, u'Win32 Executable (generic)'], [1.4, u'Win16/32 Executable Delphi generic']]
Compilation Time Stamp	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC] [SUSPICIOUS]
LegalCopyright	2015
FileVersion	4.0
CompanyName	Compusoft Hard- & Software GmbH
Comments	This installation was built with Inno Setup.
ProductName	ShopLuKaSOXID
ProductVersion	4.0
FileDescription	Artikel Abgleichsystem zu Oxid 4.x Shops
Translation	0x0000 0x04b0
Entry Point	0x40aa98 (CODE)
Machine Type	Intel 386 or later - 32Bit
File Size	4703240
Ssdeep	98304:n5S5cx58o/LlOSfNugUO58ziZkgwtIEcXSHWkUfBpdASQSUV+YHtRJqq4O:E5c/8S5ugXEYkTL41fBXQzv714O
Sha256	929b9dcfc8a43721ece5cb448cb486fbf5f5ded0f290eb1973a1ade67a1fab10
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/c/8/5/5/c85530bfd84b61f2aaad539a348d3032b934f8a2', u'EXE:ProductName': u'ShopLuKaSOXID ', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2023:07:26 19:36:35+00:00', u'EXE:InitializedDataSize': 13312, u'File:FileModifyDate': u'2023:07:26 19:36:34+00:00', u'EXE:FileVersionNumber': u'4.0.0.0', u'EXE:FileVersion': u'4.0 ', u'File:FileSize': u'4.5 MB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': u'4.0 ', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'Compusoft Hard- & Software GmbH ', u'File:FileName': u'c85530bfd84b61f2aaad539a348d3032b934f8a2', 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'2015 ', 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/c/8/5/5', u'EXE:FileDescription': u'Artikel Abgleichsystem zu Oxid 4.x Shops ', 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'2023:07:26 19:36:35+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'Neutral', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'4.0.0.0'}]
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	0x2374	0x2400	5.24117495604	7d190f730e071f82229f85f543e6873b

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': 74436, u'sha256': u'7f2b83efef7fa52c4d918fe7cd6216c7673bbe4cbbea4e931eaecee7d5044956', u'type': u'data', u'size': 2740}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 77176, u'sha256': u'2c0d32398e3c95657a577c044cc32fe24fa058d0c32e13099b26fd678de8354f', u'type': u'data', u'size': 754}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 77932, u'sha256': u'840989e0a92f2746ae60b8e3efc1a39bcca17e82df3634c1643d76141fc75bb3', u'type': u'data', u'size': 780}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 78712, u'sha256': u'26bda4da3649a575157a6466468a0a8694475664385595412 0fd715f3c9c7f78', u'type': u'data', u'size': 718}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 79432, u'sha256': u'd786490af7fe66042fb4a7d52023f5a1442f9b5e65d067b9093d1a128a6af34c', u'type': u'data', u'size': 104}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 79536, u'sha256': u'00a0794f0a493c167f64ed8b119d49bdc59f76bb35e5c295dc047095958ee2fd', u'type': u'data', u'size': 180}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 79716, u'sha256': u'34973a8a33b90ec734bd328198311f579666d5aeb04c94f469ebb822689de3c3', u'type': u'data', u'size': 174}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 79892, u'sha256':

u'6a01524c185616fe3be68ab58ce982c391cfeff1af66e3accaafcd03e33b613f', u'type': u'data', u'size': 44}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 79936, u'sha256': u'5a15635f341ecd5ad8a500c7fce6f6b4fdfecfea67e54a00906d460fdae57ab4', u'type': u'MS Windows icon resource - 1 icon, 32x27', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 79956, u'sha256': u'90710f9106f08edaedf5c393c9566f018f1cb9e54c751b0c5800d9b0876d9095', u'type': u'data', u'size': 1268}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 81224, 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