VALKYRIE COMODO

Summary

File Name: Instalar.exe

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

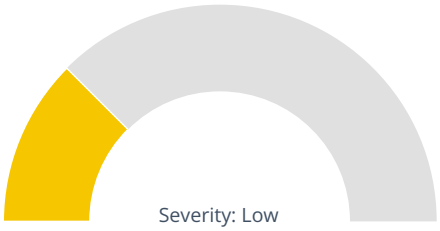
SHA1: 6ff269608201a97017590f0b7cc0081ad286ba3e

MD5: eb2906a84808343685b26df16297d100

PUA

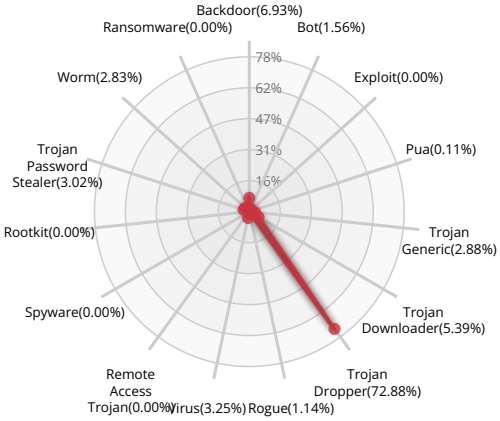
Valkyrie Final Verdict

DETECTION SECTION

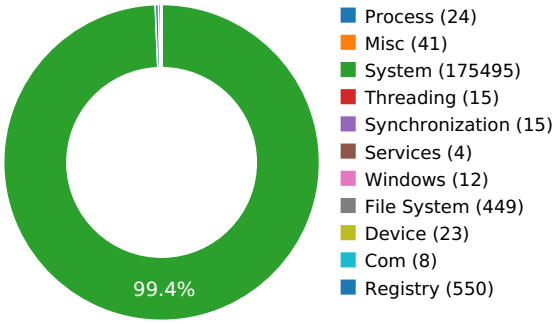


Verdict: PUA

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

The executable is compressed using UPX Show sources

INFORMATION DISCOVERY

Reads data out of its own binary image Show sources

DATA OBFUSCATION

Drops a binary and executes it Show sources

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\6ff269608201a97017590f0b7cc0081ad286ba3e.exe
C:\Windows\System32\UxTheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\6ff269608201a97017590f0b7cc0081ad286ba3e.exe.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
C:\Windows\Fonts\staticcache.dat
C:\Windows\win.ini
C:\Users\user\AppData\Local\Temp\RarSFX0
\Device\KsecDD
C:
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\RarSFX0\LOADER.EXE
C:\Users\user\AppData\Local\Temp\RarSFX0\Instalador.exe
C:\Users\user\AppData\Local\Temp\RarSFX0\INSTALAR.EXE
C:\Users\user\AppData\Local\Temp\RarSFX0\TH.EXE
C:\Users\user\AppData\Local\Temp\RarSFX0\TH01.DAT
C:\Users\user\AppData\Local\Temp\RarSFX0\TH32INS.DAT
C:\Users\user\AppData\Local\Temp\RarSFX0\TH32MAC.DAT
C:\Users\user\AppData\Local\Temp\RarSFX0\TH32.zip
C:\Users\user\AppData\Local\Temp\RarSFX0\TH59VSE.zip
C:\Users\user\AppData\Local\Temp\RarSFX0\WININET.ZIP
C:\Users\user\AppData\Local\Temp\RarSFX0\LEEME.DOC
C:\Users\user\AppData\Local\Temp\RarSFX0\DUNZIP32.DLL
C:\Users\user\AppData\Local\Temp\RarSFX0\TH32WIN.DLL
C:\Users\user\AppData\Local\Temp\RarSFX0\THD32ENG.DLL
C:\Users\user\AppData\Local\Temp\RarSFX0\THD32MAC.DLL
C:\Users\user\AppData\Local\Temp\RarSFX0\instalar.ini
C:\Users\user\AppData\Local\Temp\RarSFX0\TH59UPD.INI

\??\MountPointManager
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\RarSFX0\wdmaud.drv
C:\Windows\System32\wdmaud.drv
C:\Windows\System32\en-US\wdmaud.drv.mui
C:\Windows\System32\en-US\MMDevAPI.DLL.mui

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\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
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_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\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\AutoSuggest

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\AutoComplete\Always Use Tab
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_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave2
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave3
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave4
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave5
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave6
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave7
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave8
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave9
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi2
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi3
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi4
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi5
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi6
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi7
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi8
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\midi9
HKEY_CURRENT_USER\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm\wheel

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wdmaud.drv

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode

HKEY_LOCAL_MACHINE\SYSTEM\Setup\SystemSetupInProgress

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{a45c254e-df1c-4efd-8020-67d146a850e0},2

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{026e516e-b814-414b-83cd-856d6fef4822},2

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},2

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},6

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},1

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\CurrentVersion\MMDevices\Audio\Render\{455ff7ad-7149-49e1-9900-d5acc7fb67ed}\Properties\{1da5d803-d492-4edd-8c23-e0c0ffee7f0e},0

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Rpc\Extensions\NdrOleExtDLL

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\CurrentVersion\MMDevices\Audio\Render\{d39cf7fb-6b16-44c3-a019-e218374ed1f1}\Properties\{a45c254e-df1c-4efd-8020-67d146a850e0},2

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\CurrentVersion\MMDevices\Audio\Render\{d39cf7fb-6b16-44c3-a019-e218374ed1f1}\Properties\{026e516e-b814-414b-83cd-856d6fef4822},2

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\CurrentVersion\MMDevices\Audio\Render\{d39cf7fb-6b16-44c3-a019-e218374ed1f1}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},2

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\CurrentVersion\MMDevices\Audio\Render\{d39cf7fb-6b16-44c3-a019-e218374ed1f1}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},6

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\CurrentVersion\MMDevices\Audio\Render\{d39cf7fb-6b16-44c3-a019-e218374ed1f1}\Properties\{b3f8fa53-0004-438e-9003-51a46e139bfc},1

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\CurrentVersion\MMDevices\Audio\Render\{d39cf7fb-6b16-44c3-a019-e218374ed1f1}\Properties\{1da5d803-d492-4edd-8c23-e0c0ffee7f0e},0

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\CurrentVersion\MMDevices\Audio\Capture\{8afafb6a-f1b0-4935-be8a-5894d19191bd}\Properties\{a45c254e-df1c-4efd-8020-67d146a850e0},2

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\RarSFX0\LOADER.EXE

C:\Users\user\AppData\Local\Temp\RarSFX0\Instalador.exe

C:\Users\user\AppData\Local\Temp\RarSFX0\INSTALAR.EXE

C:\Users\user\AppData\Local\Temp\RarSFX0\TH.EXE

C:\Users\user\AppData\Local\Temp\RarSFX0\TH01.DAT

C:\Users\user\AppData\Local\Temp\RarSFX0\TH32INS.DAT

C:\Users\user\AppData\Local\Temp\RarSFX0\TH32MAC.DAT

C:\Users\user\AppData\Local\Temp\RarSFX0\TH32.zip

C:\Users\user\AppData\Local\Temp\RarSFX0\TH59VSE.zip

C:\Users\user\AppData\Local\Temp\RarSFX0\WININET.ZIP

C:\Users\user\AppData\Local\Temp\RarSFX0\LEEME.DOC
C:\Users\user\AppData\Local\Temp\RarSFX0\DUNZIP32.DLL
C:\Users\user\AppData\Local\Temp\RarSFX0\TH32WIN.DLL
C:\Users\user\AppData\Local\Temp\RarSFX0\THD32ENG.DLL
C:\Users\user\AppData\Local\Temp\RarSFX0\THD32MAC.DLL
C:\Users\user\AppData\Local\Temp\RarSFX0\instalar.ini
C:\Users\user\AppData\Local\Temp\RarSFX0\TH59UPD.INI

RESOLVED APIS

kernel32.dll.CloseHandle
kernel32.dll.CompareStringA
kernel32.dll.CreateDirectoryA
kernel32.dll.CreateDirectoryW
kernel32.dll.CreateFileA
kernel32.dll.CreateFileW
kernel32.dll.DeleteFileA
kernel32.dll.DeleteFileW
kernel32.dll.DosDateTimeToFileTime
kernel32.dll.ExitProcess
kernel32.dll.ExpandEnvironmentStringsA
kernel32.dll.FileTimeToLocalFileTime
kernel32.dll.FileTimeToSystemTime
kernel32.dll.FindClose
kernel32.dll.FindFirstFileA
kernel32.dll.FindFirstFileW
kernel32.dll.FindNextFileA
kernel32.dll.FindNextFileW
kernel32.dll.FindResourceA
kernel32.dll.FreeLibrary
kernel32.dll.GetCPInfo
kernel32.dll.GetCommandLineA
kernel32.dll.GetCurrentDirectoryA
kernel32.dll.GetCurrentProcess
kernel32.dll.GetDateFormatA
kernel32.dll.GetFileAttributesA

kernel32.dll.GetFileAttributesW
kernel32.dll.GetFileType
kernel32.dll.GetFullPathNameA
kernel32.dll.GetLastError
kernel32.dll.GetLocaleInfoA
kernel32.dll.GetModuleFileNameA
kernel32.dll.GetModuleHandleA
kernel32.dll.GetNumberFormatA
kernel32.dll.GetProcAddress
kernel32.dll.GetProcessHeap
kernel32.dll.GetStdHandle
kernel32.dll.GetTempPathA
kernel32.dll.GetTickCount
kernel32.dll.GetTimeFormatA
kernel32.dll.GetVersionExA
kernel32.dll.GlobalAlloc
kernel32.dll.HeapAlloc
kernel32.dll.HeapFree
kernel32.dll.HeapReAlloc
kernel32.dll.IsDBCSLeadByte
kernel32.dll.LoadLibraryA
kernel32.dll.LocalFileTimeToFileTime
kernel32.dll.MoveFileA
kernel32.dll.MoveFileExA
kernel32.dll.MultiByteToWideChar
kernel32.dll.ReadFile
kernel32.dll.SetCurrentDirectoryA
kernel32.dll.SetEndOfFile
kernel32.dll.SetEnvironmentVariableA
kernel32.dll.SetFileAttributesA
kernel32.dll.SetFileAttributesW
kernel32.dll.SetFilePointer
kernel32.dll.SetFileTime
kernel32.dll.SetLastError
kernel32.dll.Sleep

kernel32.dll.SystemTimeToFileTime
kernel32.dll.WaitForSingleObject
kernel32.dll.WideCharToMultiByte
kernel32.dll.WriteFile
kernel32.dll.lstrcmpiA
kernel32.dll.lstrlenA
advapi32.dll.AdjustTokenPrivileges
advapi32.dll.LookupPrivilegeValueA
advapi32.dll.OpenProcessToken
advapi32.dll.RegCloseKey
advapi32.dll.RegCreateKeyExA
advapi32.dll.RegOpenKeyExA
advapi32.dll.RegQueryValueExA
advapi32.dll.RegSetValueExA
advapi32.dll.SetFileSecurityA

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\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\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_CURRENT_USER
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
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\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_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\6ff269608201a97017590f0b7cc0081ad286ba3e.exe
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_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\DRIVERS32
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave2
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave3
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave4
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave5
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave6
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DRIVERS32\wave7

READ FILES

C:\Users\user\AppData\Local\Temp\6ff269608201a97017590f0b7cc0081ad286ba3e.exe
C:\Windows\System32\UxTheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Windows\Fonts\staticcache.dat
C:\Windows\win.ini
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\RarSFX0\LOADER.EXE

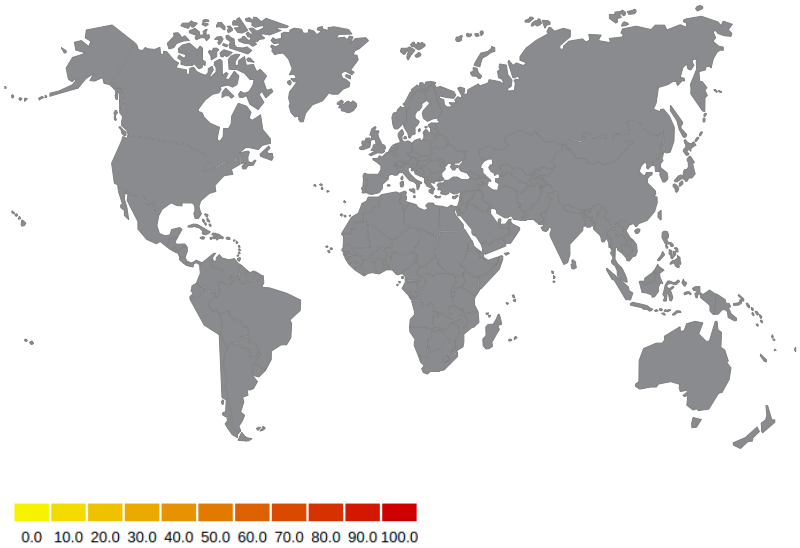
C:\Users\user\AppData\Local\Temp\RarSFX0\Instalador.exe
C:\Users\user\AppData\Local\Temp\RarSFX0\INSTALAR.EXE
C:\Users\user\AppData\Local\Temp\RarSFX0\TH.EXE
C:\Users\user\AppData\Local\Temp\RarSFX0\TH01.DAT
C:\Users\user\AppData\Local\Temp\RarSFX0\TH32INS.DAT
C:\Users\user\AppData\Local\Temp\RarSFX0\TH32MAC.DAT
C:\Users\user\AppData\Local\Temp\RarSFX0\TH32.zip
C:\Users\user\AppData\Local\Temp\RarSFX0\TH59VSE.zip
C:\Users\user\AppData\Local\Temp\RarSFX0\WININET.ZIP
C:\Users\user\AppData\Local\Temp\RarSFX0\LEEME.DOC
C:\Users\user\AppData\Local\Temp\RarSFX0\DUNZIP32.DLL
C:\Users\user\AppData\Local\Temp\RarSFX0\TH32WIN.DLL
C:\Users\user\AppData\Local\Temp\RarSFX0\THD32ENG.DLL
C:\Users\user\AppData\Local\Temp\RarSFX0\THD32MAC.DLL
C:\Users\user\AppData\Local\Temp\RarSFX0\instalar.ini
C:\Users\user\AppData\Local\Temp\RarSFX0\TH59UPD.INI
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\System32\en-US\wdmaud.drv.mui
C:\Windows\System32\en-US\MMDevAPI.DLL.mui

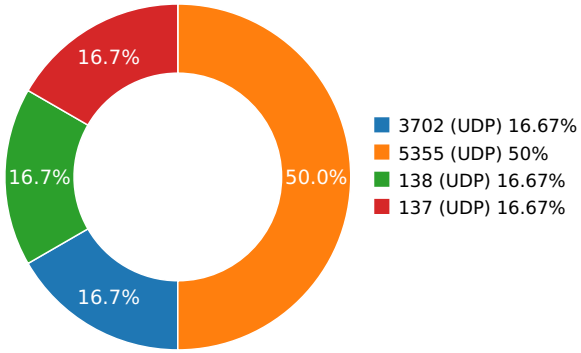
MUTEXES

CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

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
6.7940261364	Sandbox	224.0.0.252	5355
6.80330204964	Sandbox	224.0.0.252	5355
6.82012009621	Sandbox	192.168.56.255	137
6.89467096329	Sandbox	239.255.255.250	3702
9.36551308632	Sandbox	224.0.0.252	5355
12.8314480782	Sandbox	192.168.56.255	138

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\RarSFX0\TH32INS.DAT	**Type :** data **MD5 :** 787270460a77d645dc972c3317160663 **SHA-1 :** e2237451ac85f1734fa2a177b3a894212de08249 **SHA-256 :** a408e96010e4f1d22457260b2a55210914b7ede **SHA-512 :** 2a42414227d6805e3b306663402d34bdb068f44 **Size :** 0.33 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\DUNZIP32.DLL	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 065fa28a93891cc1afb45281aa74beb9 **SHA-1 :** c95ae064d452f9566c1711c75df558c20c2fab4f **SHA-256 :** 81e2e0211293ed9df8611e1132ea814c5c87696f **SHA-512 :** b333b7f0928ef559e2e5db25ac66b54e7c040c3f **Size :** 74.24 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\TH59UPD.INI	**Type :** ISO-8859 text, with CRLF line terminators **MD5 :** 35fefba2e08343cae7cee8dd49a306d0 **SHA-1 :** 59ee14341fbb4fa0e550a294aff70cdd471d78a3 **SHA-256 :** b728abaeae19aa783e29d45ff62f23647b702ffca **SHA-512 :** ff3d0c97d1c34cc184daa170405d170bbcabeef27 **Size :** 0.627 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\Instalar.Ini	**Type :** ISO-8859 text, with CRLF line terminators **MD5 :** 0b108f0f62bc562be581e582dce3f8e0 **SHA-1 :** 72135ee491a524570b3385452e4fd678574af049 **SHA-256 :** 49d98dbcad01052c751c0ea7f6b1105285963a19 **SHA-512 :** 18c333f54036b46e326410eef4c46f1cd38bc19ac **Size :** 6.783 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\LOADER.EXE	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 45dcdf39418293fde2cc06ae301f8d4a **SHA-1 :** e208824af6842fd347e02284c1c69babaccc9324 **SHA-256 :** 147f778cbe11fc64d406cfae3f3284e9d5fc309fc4 **SHA-512 :** 390dccdd746679b282c411d523d56e02de2a198 **Size :** 372.224 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\TH59VSE.Zip	**Type :** Zip archive data, at least v2.0 to extract **MD5 :** ac4f9c015340d32017cfc326e6f6bb24 **SHA-1 :** c62cbe8c0a2f64de540a0698f9818e40a1488761 **SHA-256 :** 26446c637cf3042d3b2ea10c3fdb2bee982fbc5cf **SHA-512 :** 8f54dab7d78b009fff50c7013e1b29edebc939a39 **Size :** 399.67 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\TH32WIN.DLL	**Type :** RAR archive data, v57, **MD5 :** d0f3a06309f3e4b08f52fe2ce7b1e4de **SHA-1 :** 16bc82798d9c43d330991918de0bf0b7a9dbea1d **SHA-256 :** edac521b0bc0570ce7ab3d95c7addba76dbc967 **SHA-512 :** 8e11d9bee8fab957ccfb4d2e0722cdadbd659591 **Size :** 0.472 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\WININET.ZIP	**Type :** Zip archive data, at least v2.0 to extract **MD5 :** eae4be7fd69256ad9ab4c95ef045b941 **SHA-1 :** 16d49c299ed16fffeca19e518b2e1bb6f0a80690 **SHA-256 :** 10cb45e264cefd3c1238ac44a930582a731a8b64 **SHA-512 :** e40b0a1eca4042b5064f4fdea694edd7db4e7f97 **Size :** 143.752 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\RarSFX0\LEEME.DOC	**Type :** ISO-8859 text, with CRLF line terminators **MD5 :** f293a3bc6c159a20ac33f8ed377b6081 **SHA-1 :** c92b68936ce5f9edee7809c571aaf19d296a9314 **SHA-256 :** 677cb50f13e6404af8b23f32b3df67a74ffe01ade **SHA-512 :** 8e531a12b71d1d9e6c7cd6c5eab3cf0f67477738 **Size :** 2.991 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\THD32MAC.DLL	**Type :** MS-DOS executable, NE for MS Windows 3.x (driver) **MD5 :** 6f011f8f0a367caff4d57929bbe8a4ff **SHA-1 :** ef5aba3e97c8c45fac2783f29a6d934b77c7f980 **SHA-256 :** be2372557572e885b12f138784babecf8dcf6036 **SHA-512 :** ada7de4789e1a38057820d51e2d4db2da5f0225 **Size :** 7.168 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\TH32MAC.DAT	**Type :** MS-DOS executable, MZ for MS-DOS **MD5 :** df1ba1f7835e7bd5d5655984f657e0cb **SHA-1 :** df4a433f2add63cd69719b65b3722a601d36cd78 **SHA-256 :** 8f8ea020ce8b575fb22e960589d73c18b957565e **SHA-512 :** a8751c976c7e6cda2d278af21e0f5f18b92cf229b **Size :** 8.418 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\THD32ENG.DLL	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** bf557f46d5b9c1e6a45a37f03ae67316 **SHA-1 :** 4f303f2da81fac6772f9005034617c7022c968ff **SHA-256 :** e4cf49467cc66538e1a0dae2922f11b86538d55a **SHA-512 :** 0f76b27b8d18d81ad7f4092199f86af57deaf8939 **Size :** 36.864 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\INSTALAR.EXE	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** dc3ce1bbfee339d83981c23c79bbdd99 **SHA-1 :** 1fb6cf5a6c9723f8726bdaa88bead06f83a1719d **SHA-256 :** 8f3e898c004f4fa7e9d08e7d6f88f3f46739e7aa27 **SHA-512 :** d8305fb3e0386d19ef1361b9e9cd041b4e793ecb **Size :** 123.904 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\TH01.DAT	**Type :** data **MD5 :** ff35aa0284a4e82f570b3cc8e93ffa86 **SHA-1 :** 14f655884d5addd223441873b7544cdd4968b68a **SHA-256 :** 065d52b76dc65e9fce4cdae670519752eea859dc **SHA-512 :** 939688c8e8f6c1b5ab2e11fe9d33027607451689 **Size :** 718.852 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\TH32.Zip	**Type :** Zip archive data, at least v2.0 to extract **MD5 :** 4c64fa8fade86a9d387c41e564a68a8b **SHA-1 :** 6018fbc7f1e4f83a1f2a72773e0e2d25058a1608 **SHA-256 :** a94ed7df0bbe3440e6b24df2b7c3237bd0cba6d **SHA-512 :** 789d33accf174546816f8543f0654cc36bc0a9046 **Size :** 1206.949 Kilobytes.
C:\Users\User\AppData\Local\Temp\RarSFX0\Instalador.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 1e522e2825a4183f546f21f5d52f9ed9 **SHA-1 :** c56d7a0e4283ae33c20ea2410a368e7e0a3956ec **SHA-256 :** 4654bdf1bb5b59445b3f5bd85efebaaa0e7aaff4 **SHA-512 :** 2039d38466661697de5662fe95d73b585a0849e **Size :** 29.184 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\RarSFX0\TH.EXE	**Type :** MS-DOS executable, MZ for MS-DOS **MD5 :** 5c468fe8413e1e1362dcd52095962c93 **SHA-1 :** 8dd743a855d90b9ffa698d1542d7ad91adeb0a72 **SHA-256 :** 92dcf63f9131c1621ba16223d279dbd888cf8597 **SHA-512 :** 2a12f9194e3f4d83ae647b5563cf86d6c5ac0dc5c **Size :** 300.713 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	Instalar.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1:	6ff269608201a97017590f0b7cc0081ad286ba3e
MD5:	eb2906a84808343685b26df16297d100
First Seen Date:	2023-06-27 17:03:10.719205 (2 years ago)
Number Of Clients Seen:	4
Last Analysis Date:	2023-06-29 16:16:47.866464 (2 years ago)
Human Expert Analysis Date:	2023-06-28 07:21:26.327168 (2 years ago)
Human Expert Analysis Result:	PUA

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	3
Trid	[]
Compilation Time Stamp	0x413F0E68 [Wed Sep 8 13:51:36 2004 UTC]
Entry Point	0x421bd0 (UPX1)
Machine Type	Intel 386 or later - 32Bit
File Size	3248109
Ssdeep	
Sha256	050849679304b4de8f0ea9e3af46b33ff7d4168c29abd405bcd54c8f7419fe0d
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
UPX0	0x1000	0x16000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
UPX1	0x17000	0xb000	0xae00	7.89941387	f76adac890590d78dae0bcf4520cc48d
.rsrc	0x22000	0x2000	0x1c00	2.87689799924	7fe8f62cbeee9826b9f629e4529c61a0

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 115804, u'sha256': u'6779dfe0887f2f559060cae82e0f30b2a1a47680c055acd12ea298d70907d8b2', u'type': u'data', u'size': 2998}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 140384, u'sha256': u'4436650a65c64265abf4b8726a33b15c2b2039fc65e120c7173bcba67feb852b', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 140684, u'sha256': u'deca6582a186b04c7305a75271b551bb736856a4f275d27ed19ccd7a146e0a2b', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 142072, u'sha256': u'513604c79e3a2d658ef87a7954c8c2ad3e3b834be401aeb1b10896370bceea33', u'type': u'data', u'size': 744}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 142820, u'sha256': u'4909357f7b991171d085d19335d65d6cc5fa36e5447f5b1cd9094dd53e3a175b', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 2216}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 123444, u'sha256': u'74b21150f7ba52e6ef93053e0baaf6fc625ce2bbedb55f9a6351d397586307f9', u'type': u'data', u'size': 698}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 124144, u'sha256': u'1559374c4030da735ce408d4a3d5f4d6de311b40ab16a1adc1f0d43b6fae9ea4', u'type': u'data', u'size': 330}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 124476, u'sha256': u'2503aa289c4512996b24db5f836731eb36e35aba956d429e52f1f79e3776de4e', u'type': u'data', u'size': 238}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 124716, u'sha256': u'f7fe29e0c76dfa30c64e57bb5aba534eadd902b25f5b97a551bad4903314dfc6', u'type': u'data', u'size': 326}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 125044, u'sha256': u'2cb7a7b5cbdac8562012d8c92099d824ccee23f4dcf9e8ddb71c3cee5e0b5a2a', u'type': u'data', u'size': 816}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 125860, u'sha256': u'650f4e32c771da63ca5e540ef37cdbe97c9fd97c298533ce3d932d583fdfb487', u'type': u'data', u'size': 566}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 126428, u'sha256': u'11e24a06b916fd00de06fe94ac10e99d5f284a4c5710e567f026eb9d450f372e', u'type': u'data', u'size': 656}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 127084, u'sha256': u'3290835dac71de52ca55727726a14bb8dba2eb2603399cfac351b103072c6e22', u'type': u'data', u'size': 998}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 128084, u'sha256': u'd7d18172fd2c45d6d88c1d886bd1a5e1ca03ee2d57b387ab2ff4b58187e91923', u'type': u'data', u'size': 650}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 128736, u'sha256': u'7482eb3f635ca980974344d85b051670a9b686cca3c104cc3cbe4cd3132d5023', u'type': u'data', u'size': 646}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 145040, u'sha256': u'8501cadee21dab1e82414ae8cf88bb1567fc47c8879ffbf8677dfd6a1d676534', u'type': u'MS Windows icon resource - 4 icons, 16x16, 16 colors', u'size': 62}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 145108, u'sha256': u'15324e5059af9c43aa7112792329216902d5821bb49bb206b71c25d9c6cd0b6a', u'type': u'XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators', u'size': 531}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS