VALKYRIE COMODO

Summary

File Name: SimplyWatch_3142637754.exe

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

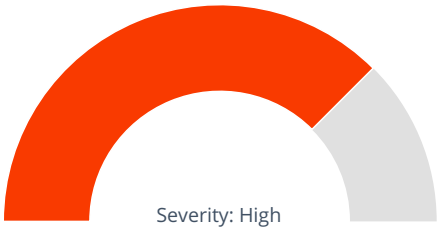
SHA1: 61adaa1e33defc6220507b83b910c562c63f014c

MD5: 332d9f2a17a88c50be5910c449fb6317

MALWARE

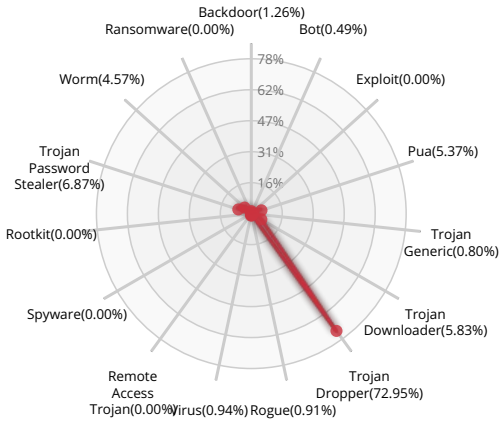
Valkyrie Final Verdict

DETECTION SECTION

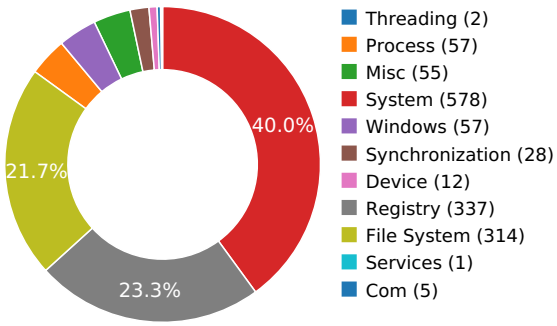


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

INFORMATION DISCOVERY

Reads data out of its own binary image Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

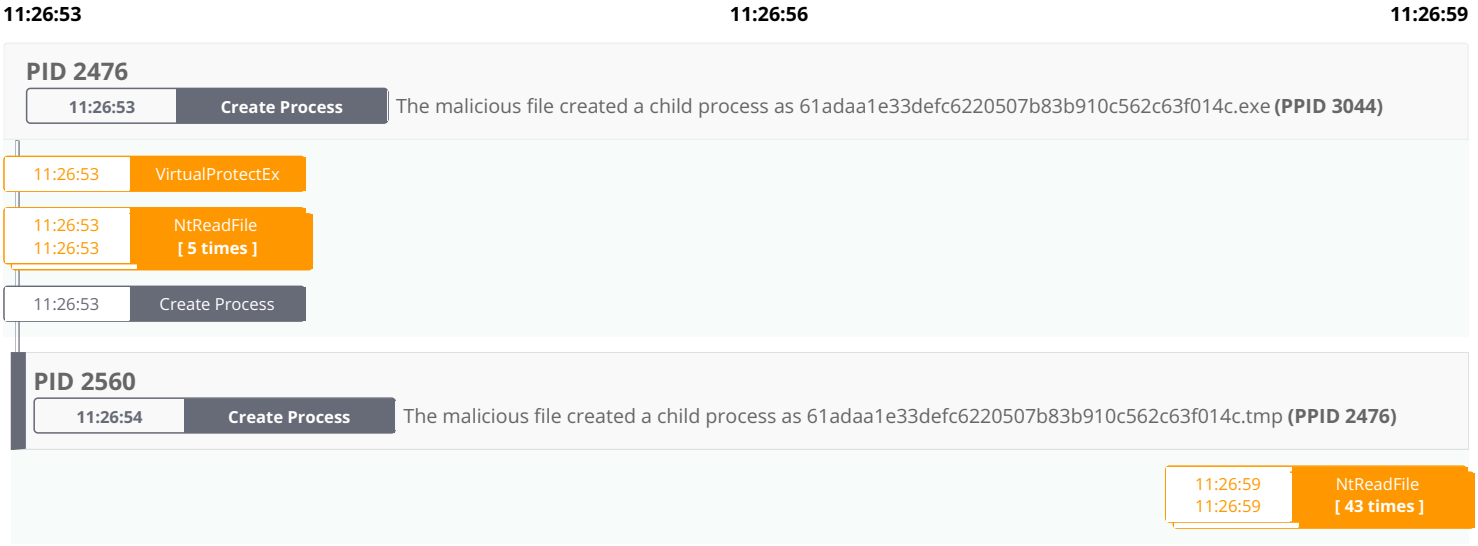
Creates RWX memory Show sources

DATA OBFUSCATION

Drops a binary and executes it Show sources

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\61adaa1e33defc6220507b83b910c562c63f014c.exe
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\is-0KU8E.tmp
C:\Users\user\AppData\Local\Temp\is-0KU8E.tmp\61adaa1e33defc6220507b83b910c562c63f014c.tmp
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Fonts\staticcache.dat
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\is-0KU8E.tmp\netmsg.dll
C:\Users\user\AppData\Local\Temp\is-JC7D7.tmp
C:\Users\user\AppData\Local\Temp\is-JC7D7.tmp_isetup
C:\Users\user\AppData\Local\Temp\is-JC7D7.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-JC7D7.tmp_isetup_shfoldr.dll
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\is-0KU8E.tmp\61adaa1e33defc6220507b83b910c562c63f014c.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:\
C:\Program Files (x86)\Rigi\
C:\Program Files (x86)\
C:\Program Files (x86)\Rigi
C:\Program Files (x86)\Rigi\Lanutet.exe
C:\Windows\System32
C:\Program Files (x86)
C:\Program Files (x86)\Rigi\unins???.*
C:\Program Files (x86)\Rigi\unins000.dat
C:\Windows\winsxs\FileMaps\program_files_x86_rigi_32387ed964e6ec49.cdf-ms

C:\Program Files (x86)\Rigi\unins000.exe
C:\Program Files (x86)\Rigi\is-VRTFQ.tmp
C:\Program Files (x86)\Rigi\Hohonire.wma
C:\Program Files (x86)\Rigi\is-TB9S0.tmp
C:\Program Files (x86)\Rigi\Celiditufo.com
C:\Program Files (x86)\Rigi\is-T45L4.tmp
C:\Program Files (x86)\Rigi\is-O0E01.tmp
C:\Program Files (x86)\Rigi\Tatokerulon.pptx
C:\Program Files (x86)\Rigi\is-92IOP.tmp
C:\Program Files (x86)\Rigi\Hebuborahabu.ha
C:\Program Files (x86)\Rigi\is-KVPVP.tmp
C:\Program Files (x86)\Rigi\Nabonepugak.pebe
C:\Program Files (x86)\Rigi\is-G1IR4.tmp
C:\Users\user\AppData\Local\Temp\is-JC7D7.tmp*
C:\Users\user\AppData\Local\Temp\is-JC7D7.tmp_isetup*

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
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\B6C2FB48
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\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_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\PendingFileRenameOperations
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\PendingFileRenameOperations2
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFiles0000

HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFiles0001
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFilesHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegSvcs0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegProcs0000
HKEY_LOCAL_MACHINE\SYSTEM\Setup\SystemSetupInProgress
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Rigi\unins000.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Rigi\Hohonire.wma
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Rigi\Celiditufo.com
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Rigi\Lanutet.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Rigi\Tatokerulon.pptx
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Rigi\Hebuborahabu.ha
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\PnpLockdownFiles\%SystemDrive%\Program Files (x86)\Rigi\Nabonepugak.pebe
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\JSCount
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\ESCount
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RRCount

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\is-0KU8E.tmp\61adaa1e33defc6220507b83b910c562c63f014c.tmp
C:\Users\user\AppData\Local\Temp\is-JC7D7.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-JC7D7.tmp_isetup_shfoldr.dll
C:\Program Files (x86)\Rigi\Lanutet.exe
C:\Program Files (x86)\Rigi\unins000.dat
C:\Program Files (x86)\Rigi\is-VRTFQ.tmp
C:\Program Files (x86)\Rigi\unins000.exe
C:\Program Files (x86)\Rigi\is-TB9S0.tmp
C:\Program Files (x86)\Rigi\Hohonire.wma
C:\Program Files (x86)\Rigi\is-T45L4.tmp
C:\Program Files (x86)\Rigi\Celiditufo.com
C:\Program Files (x86)\Rigi\is-O0E01.tmp
C:\Program Files (x86)\Rigi\is-92IOP.tmp
C:\Program Files (x86)\Rigi\Tatokerulon.pptx
C:\Program Files (x86)\Rigi\is-KVPVP.tmp
C:\Program Files (x86)\Rigi\Hebuborahabu.ha
C:\Program Files (x86)\Rigi\is-G1IR4.tmp
C:\Program Files (x86)\Rigi\Nabonepugak.pebe

RESOLVED APIS

kernel32.dll.SetDllDirectoryW
kernel32.dll.SetSearchPathMode
kernel32.dll.SetProcessDEPPolicy
kernel32.dll.Wow64DisableWow64FsRedirection
kernel32.dll.Wow64RevertWow64FsRedirection
kernel32.dll.GetUserDefaultUILanguage
kernel32.dll.AreFileApisANSI
kernel32.dll.GetCurrentProcessId
kernel32.dll.GetModuleFileNameW
kernel32.dll.CreateFileW
kernel32.dll.VirtualAlloc
kernel32.dll.LoadLibraryA
kernel32.dll.VirtualProtect
kernel32.dll.VirtualFree
kernel32.dll.FreeLibrary
kernel32.dll.DeleteCriticalSection
kernel32.dll.LeaveCriticalSection
kernel32.dll.EnterCriticalSection
kernel32.dll.InitializeCriticalSection
kernel32.dll.LocalFree
kernel32.dll.LocalAlloc
kernel32.dll.GetCurrentThreadId
kernel32.dll.WideCharToMultiByte
kernel32.dll.lstrlenA
kernel32.dll.lstrcpynA
kernel32.dll.LoadLibraryExA
kernel32.dll.GetThreadLocale
kernel32.dll.GetStartupInfoA
kernel32.dll.GetProcAddress
kernel32.dll.GetModuleHandleA
kernel32.dll.GetModuleFileNameA
kernel32.dll.GetLocaleInfoA
kernel32.dll.GetCommandLineA

kernel32.dll.FindFirstFileA
kernel32.dll.FindClose
kernel32.dll.ExitProcess
kernel32.dll.WriteFile
kernel32.dll.UnhandledExceptionFilter
kernel32.dll.RtlUnwind
kernel32.dll.RaiseException
kernel32.dll.GetStdHandle
user32.dll.GetKeyboardType
user32.dll.LoadStringA
user32.dll.MessageBoxA
user32.dll.CharNextA
advapi32.dll.RegQueryValueExA
advapi32.dll.RegOpenKeyExA
advapi32.dll.RegCloseKey
oleaut32.dll.SysFreeString
oleaut32.dll.SysReAllocStringLen
kernel32.dll.TlsSetValue
kernel32.dll.TlsGetValue
kernel32.dll.TlsFree
kernel32.dll.TlsAlloc
kernel32.dll.VirtualQueryEx
kernel32.dll.VirtualQuery
kernel32.dll.ReadProcessMemory
kernel32.dll.OpenProcess
kernel32.dll.MoveFileExA
kernel32.dll.GetVersionExA
kernel32.dll.GetTickCount
kernel32.dll.GetSystemPowerStatus
kernel32.dll.GetSystemInfo
kernel32.dll.GetStringTypeExA
kernel32.dll.GetDiskFreeSpaceA
kernel32.dll.GetCurrencyFormatW
kernel32.dll.GetCPInfo
kernel32.dll.GetACP

kernel32.dll.FillConsoleOutputCharacterA
kernel32.dll.EnumCalendarInfoA
kernel32.dll.CloseHandle
user32.dll.GetUserObjectInformationA
user32.dll.GetSystemMetrics
user32.dll.GetLastInputInfo
user32.dll.AppendMenuA
kernel32.dll.GetDiskFreeSpaceExA

DELETED FILES

C:\Users\user\AppData\Local\Temp\is-0KU8E.tmp\61adaa1e33defc6220507b83b910c562c63f014c.tmp
C:\Users\user\AppData\Local\Temp\is-0KU8E.tmp
C:\Program Files (x86)\Rigi\is-VRTFQ.tmp
C:\Program Files (x86)\Rigi\is-TB9S0.tmp
C:\Program Files (x86)\Rigi\is-T45L4.tmp
C:\Program Files (x86)\Rigi\is-O0E01.tmp
C:\Program Files (x86)\Rigi\is-92IOP.tmp
C:\Program Files (x86)\Rigi\is-KVPVP.tmp
C:\Program Files (x86)\Rigi\is-G1IR4.tmp
C:\Users\user\AppData\Local\Temp\is-JC7D7.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-JC7D7.tmp_isetup_shfoldr.dll
C:\Users\user\AppData\Local\Temp\is-JC7D7.tmp_isetup
C:\Users\user\AppData\Local\Temp\is-JC7D7.tmp

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFilesHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFiles0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_CURRENT_USER\Software\Borland\Locales
HKEY_LOCAL_MACHINE\Software\Borland\Locales
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales
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\61adaa1e33defc6220507b83b910c562c63f014c.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\B6C2FB48
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\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

READ FILES

C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Windows\System32\netmsg.dll
C:\Users\user\AppData\Local\Temp\61adaa1e33defc6220507b83b910c562c63f014c.exe
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Fonts\staticcache.dat
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\is-JC7D7.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-JC7D7.tmp_isetup_shfoldr.dll
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Windows\System32\imageres.dll
C:\Windows\System32\shell32.dll
C:\
C:\Program Files (x86)\Rigi\Lanutet.exe
C:\Program Files (x86)\Rigi\unins000.dat
C:\Windows\winsxs\FileMaps\program_files_x86_rigi_32387ed964e6ec49.cdf-ms
C:\Program Files (x86)\Rigi\is-VRTFQ.tmp
C:\Users\user\AppData\Local\Temp\is-0KU8E.tmp\61adaa1e33defc6220507b83b910c562c63f014c.tmp
C:\Program Files (x86)\Rigi\is-TB9S0.tmp
C:\Program Files (x86)\Rigi\is-T45L4.tmp
C:\Program Files (x86)\Rigi\is-O0E01.tmp
C:\Program Files (x86)\Rigi\is-92IOP.tmp
C:\Program Files (x86)\Rigi\is-KVPVP.tmp
C:\Program Files (x86)\Rigi\is-G1IR4.tmp

MUTEXES

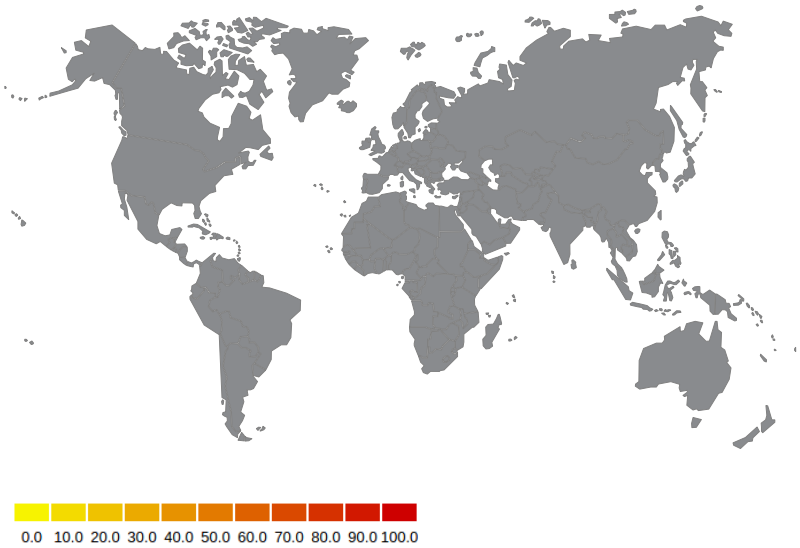
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000
DefaultTabtip-MainUI

MODIFIED REGISTRY KEYS

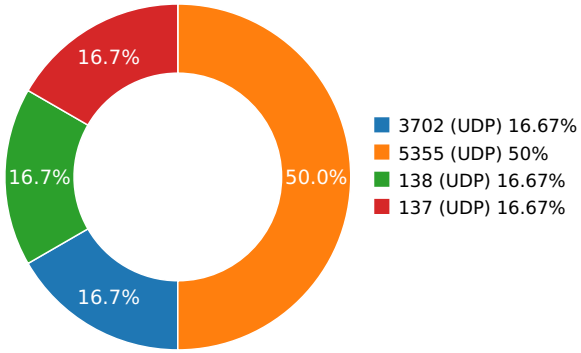
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFiles0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\RegFilesHash
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1\Inno Setup: Setup Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1\Inno Setup: App Path
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1\InstallLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1\Inno Setup: Icon Group
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1\Inno Setup: User
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1\Inno Setup: Language
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1\QuietUninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1\DisplayVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1\NoModify
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1\NoRepair
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1\InstallDate
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1\MajorVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1\MinorVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Rigi_is1\EstimatedSize

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
3.20455503464	Sandbox	192.168.56.255	137
3.24753117561	Sandbox	224.0.0.252	5355
3.29523801804	Sandbox	224.0.0.252	5355
3.63512706757	Sandbox	239.255.255.250	3702
5.87788701057	Sandbox	224.0.0.252	5355
9.27802205086	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Rigi\Tatokerulon.Pptx	**Type :** data **MD5 :** 34b49ee2bd4ce5f7a7f75a3a32c345cb **SHA-1 :** fb1c23e02ae58f1f22c9bdf45a246afba9e9c745 **SHA-256 :** 757e0d37f39b46ec93f8721affa08e157e38c0f064 **SHA-512 :** d7077160943608f1b0fe2d3bb56473078065372 **Size :** 21.671 Kilobytes.
C:\Program Files (X86)\Rigi\Celiditufo.Com	**Type :** data **MD5 :** 771f1826862de243fcbed941fc542f7a **SHA-1 :** bb934f9160a2d6f6fcc5bdd5714c9fea115992f7 **SHA-256 :** a093af4a9003a299581fa56306749f0a42a67e51 **SHA-512 :** a445dd7e1bfe92075d35993626acb82543a5514 **Size :** 22.157 Kilobytes.
C:\Program Files (X86)\Rigi\Unins000.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 806678325c4de0c1fbfc56726432a65d **SHA-1 :** 8ebba41a1a34326e2e41ff054bbb299077138f28 **SHA-256 :** 2b2e13de0eeebf0354f2cffed0797ca49c50d18f5 **SHA-512 :** 6dd884c4e81e3292063eeb47e78efb712890b3ef **Size :** 715.253 Kilobytes.
C:\Program Files (X86)\Rigi\Unins000.Dat	**Type :** data **MD5 :** 3fa67c9811fe51fd24e9804263ca5b84 **SHA-1 :** c036207523b0903ce551aae4362c94f2ee359543 **SHA-256 :** 9e0442d6d5e32dc73d30f6f0c73130e3232d598d **SHA-512 :** 3e617bfc71dba49d2be1fb1db58607052c5134d7 **Size :** 1.158 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-JC7D7.Tmp_isetup_shfoldr.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** 92dc6ef532fbb4a5c3201469a5b5eb63 **SHA-1 :** 3e89ff837147c16b4e41c30d6c796374e0b8e62c **SHA-256 :** 9884e9d1b4f8a873ccbd81f8ad0ae257776d2348 **SHA-512 :** 9908e573921d5dbc3454a1c0a6c969ab8a81cc2e **Size :** 23.312 Kilobytes.
C:\Program Files (X86)\Rigi\Hohonire.Wma	**Type :** data **MD5 :** 089eb4835ccca07ecce0bd44b2747cfb **SHA-1 :** fe08d82e65c610eea63353dc193decdb3eb1f7e3 **SHA-256 :** ff0df554eb9831edb98e0f4ecc8e42f5ae5b6b8c6 **SHA-512 :** 0392d77f0b77d5e43bcf5996592582e2cf395136 **Size :** 22.593 Kilobytes.
C:\Program Files (X86)\Rigi\Lanutet.Exe	**Type :** data **MD5 :** 1a1212ba48fa06a8810470db3bac5f1d **SHA-1 :** c5259d422cd63526403f01b59416dc5694c25f48 **SHA-256 :** f2e81caf10c159b1601976ea83869cd0e5ad55db **SHA-512 :** 5b5a6cbd5d1b9e37e60681cddd797c5d0d1b6df **Size :** 21.629 Kilobytes.
C:\Program Files (X86)\Rigi\Nabonepugak.Pebe	**Type :** data **MD5 :** 5aa091b1705e61658037c22a21f357b3 **SHA-1 :** e69ca1d188db94b33c0dd172dbe67a827cb24de5 **SHA-256 :** bf0d41eb1c8262782bc3eb4971adfe20a643d0f6 **SHA-512 :** cdaafff3eae6b6c0a2482d366e657b8496d05869 **Size :** 22.746 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Rigi\Hebuborahabu.Ha	**Type :** data **MD5 :** 5869620bed904c29f9712fe94ac8cfe2 **SHA-1 :** 8b1c33e648ff0a9666c4b2a044d20dc321be8770 **SHA-256 :** 825ca811bd8b74976685cb852251501e65b3362 **SHA-512 :** 68f2cba1139da991b312e267b4101aa3afdd2af4 **Size :** 23.038 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-0KU8E.Tmp\61adaa1e33defc6220507b83b910c562c63f014c.Tmp	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** c49b0148cb58b886f60cb32eb5e81439 **SHA-1 :** 9c64093d08c5ea02a3622f2b616546d3c67a2360 **SHA-256 :** fc13f965789a342dba0784492c2e2797ab92bdea **SHA-512 :** 70968fa616ff38b39e9b266c38f99e4b25a749d5f **Size :** 704.0 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-JC7D7.Tmp_isetup_setup64.Tmp	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** 4ff75f505fddcc6a9ae62216446205d9 **SHA-1 :** efe32d504ce72f32e92dcf01aa2752b04d81a342 **SHA-256 :** a4c86fc4836ac728d7bd96e7915090fd59521a9e **SHA-512 :** ba0469851438212d19906d6da8c4ae95ff1c0711 **Size :** 6.144 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	SimplyWatch_3142637754.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	61adaa1e33defc6220507b83b910c562c63f014c
MD5:	332d9f2a17a88c50be5910c449fb6317
First Seen Date:	2018-03-13 00:06:56.296802 (10 months ago)
Number Of Clients Seen:	2
Last Analysis Date:	2018-03-13 00:06:56.296802 (10 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	Pecefoped
Comments	This installation was built with Inno Setup.
ProductName	Fufotofek
ProductVersion	4.2.9
FileDescription	Fufotofek Setup
Translation	0x0000 0x04b0
Entry Point	0x409c40 (CODE)
Machine Type	Intel 386 or later - 32Bit
File Size	1741118
Ssdeep	49152:Fc8CJDn+V4uEJsK80bFqJ++TRbcRQBamBcEmBDt1J:+/n+V4uEJsobkTRAUkBDp
Sha256	5c278301d2c62debbb64d86bcc552455bafd85bdda501e740a6743fdad27267c
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/6/1/a/d/61adaa1e33defc6220507b83b910c562c63f014c', u'EXE:ProductName': u'Fufotofek ', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:03:13 00:06:12+00:00', u'EXE:InitializedDataSize': 207872, u'File:FileModifyDate': u'2018:03:12 20:24:55+00:00', u'EXE:FileVersionNumber': u'0.0.0.0', u'EXE:FileVersion': u' ', u'File:FileSize': u'1700 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'4.2.9 ', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'Pecefoped ', u'File:FileName': u'61adaa1e33defc6220507b83b910c562c63f014c', 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/6/1/a/d', u'EXE:FileDescription': u'Fufotofek Setup ', u'EXE:EntryPoint': u'0x9c40', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 37888, u'EXE:Comments': u'This installation was built with Inno Setup.', u'File:FileInodeChangeDate': u'2018:03:12 20:24:55+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	884310b1928934402ea6fec1dbd3cf5e

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0x9364	0x9400	6.55663468546	25eb7e76aef06a8c6d34bcc9989d3007
DATA	0xb000	0x24c	0x400	2.73909563469	d5ea23d4ecf110fd2591314cbaa84278
BSS	0xc000	0xe88	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0xd000	0x950	0xa00	4.4307330698	bb5485bf968b970e5ea81292af2acdba
.tls	0xe000	0x8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0xf000	0x18	0x200	0.20448815744	9ba824905bf9c7922b6fc87a38b74366
.reloc	0x10000	0x8b4	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x11000	0x31bd0	0x31c00	7.01250067925	d72d1be9e53d399577bb067d7ad16237

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
    - GetUserDefaultLangID
    - GetSystemInfo
    - 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_NEUTRAL', u'name': u'RT_ICON', u'offset': 70724, u'sha256': u'9e1bdbf89860c58e5b54490f0ceb64198935047fef0a90d27bed949a659e6b03', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 71852, u'sha256': u'3580da9caf77adb6213933084947be61211f8f4a6110108f5d8036fe30ceb925', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 74292, u'sha256': u'6911bda72489fcaff39948fe10308f114d03b4201f22d98b5c18953407a62803', u'type': u'dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4269703810, next used block 4286611331', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 78556, u'sha256': u'80b996119898fa83a25fedee4fe7aaf8775ee9cfead32bf149a8875effc4c2b8', u'type': u'dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4252991872, next used block 4286283392', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 88196, u'sha256': u'4fb2a55edcb2bf9b828eed9b6ecbe8ce663b7ec3172031b8080e07999e43eab8', u'type': u'data', u'size': 13032}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 101228, u'sha256': u'5414afac691413df2ec21a80827d9b9fd3272d4656d7bde92bbffbf04a76e4c5', u'type': u'dBase IV DBT of \\200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4218976892, next used block 4202462592', u'size': 16936}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 118164, u'sha256': u'644081f07a9336396a31415b453d55bee28320ef76e4f7ed2ac5411fd4e7561c', u'type': u'dBase IV DBT of \\300.DBF, block length 36864, next

free block index 40, next free block 4286675838, next used block 4269834106', u'size': 38056}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 156220, u'sha256': u'10dc9886819e82550da64974e564e863d4c286fe5691fbe91845800731047018', u'type': u'data', u'size': 67624}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 223844, u'sha256': u'aaa8b55f3efe5182916f4621665e28eb173178f64c6f91cdec02a2308523f2f1', u'type': u'PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced', u'size': 44039}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 267884, u'sha256': u'2c0d32398e3c95657a577c044cc32fe24fa058d0c32e13099b26fd678de8354f', u'type': u'data', u'size': 754}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 268640, u'sha256': u'840989e0a92f2746ae60b8e3efc1a39bcca17e82df3634c1643d76141fc75bb3', u'type': u'data', u'size': 780}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 269420, u'sha256': u'26bda4da3649a575157a6466468a0a8694475664385595412 0fd715f3c9c7f78', u'type': u'data', u'size': 718}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 270140, u'sha256': u'd786490af7fe66042fb4a7d52023f5a1442f9b5e65d067b9093d1a128a6af34c', u'type': u'data', u'size': 104}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 270244, u'sha256': u'00a0794f0a493c167f64ed8b119d49bdc59f76bb35e5c295dc047095958ee2fd', u'type': u'data', u'size': 180}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 270424, u'sha256': u'34973a8a33b90ec734bd328198311f579666d5aeb04c94f469ebb822689de3c3', u'type': u'data', u'size': 174}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 270600, u'sha256': u'97c257cf986a29b05fd65d05f38ad613f14512025cae23aeb5558b60b3cddea0', u'type': u'data', u'size': 44}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 270644, u'sha256': u'3f5f4aa99343167f78646d883b3937ce5ab1f55eefaaea88ad07abfbd3994446', u'type': u'MS Windows icon resource - 9 icons, 16x16', u'size': 132}

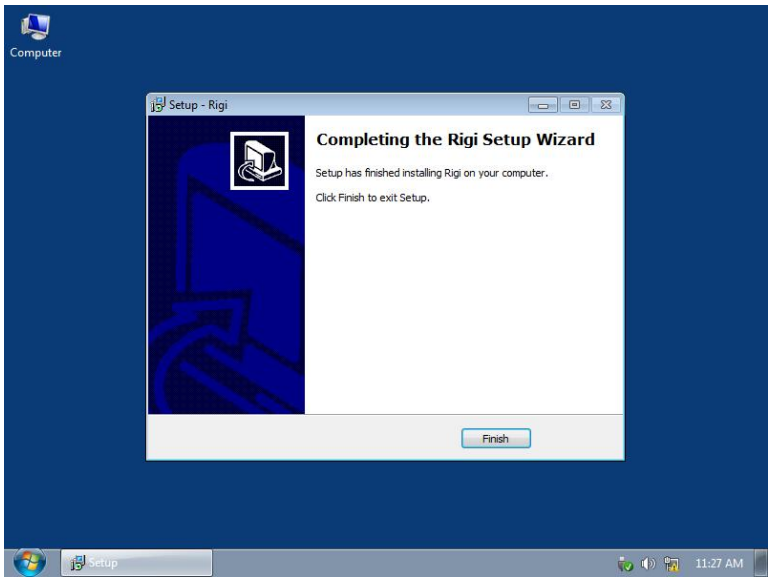
{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 270776, u'sha256': u'081ddfe65bca93858ad761d98e310ef45e34c5f0f2f2f9010a8a1e2bb37f0f98', u'type': u'COM executable for DOS', u'size': 1208}

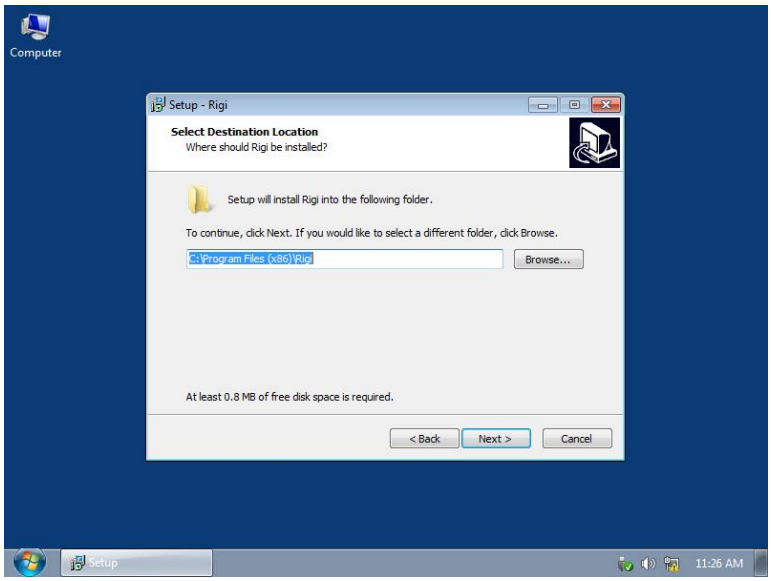
{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 271984, u'sha256': u'ec233469005d39f4f2673be991a0415318631a59c5976c35d4dd22db45226fd0', u'type': u'XML 1.0 document, ASCII text, with CRLF line terminators', u'size': 1376}

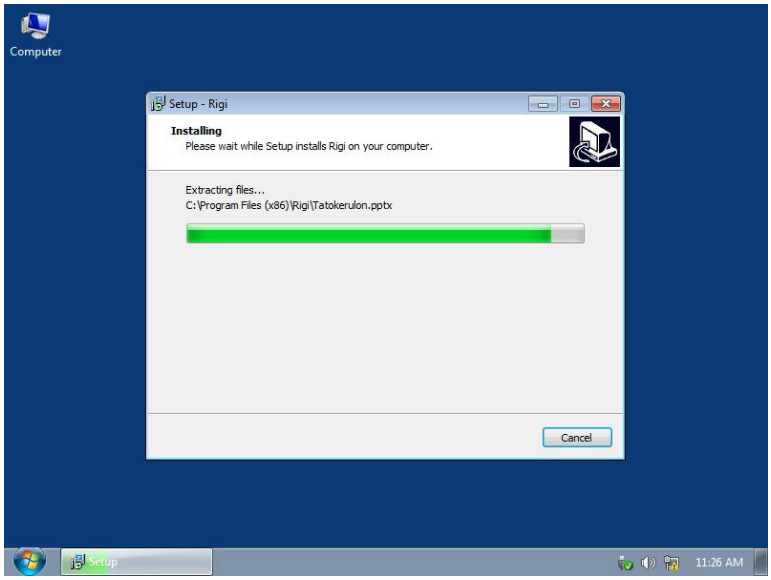
CERTIFICATE VALIDATION

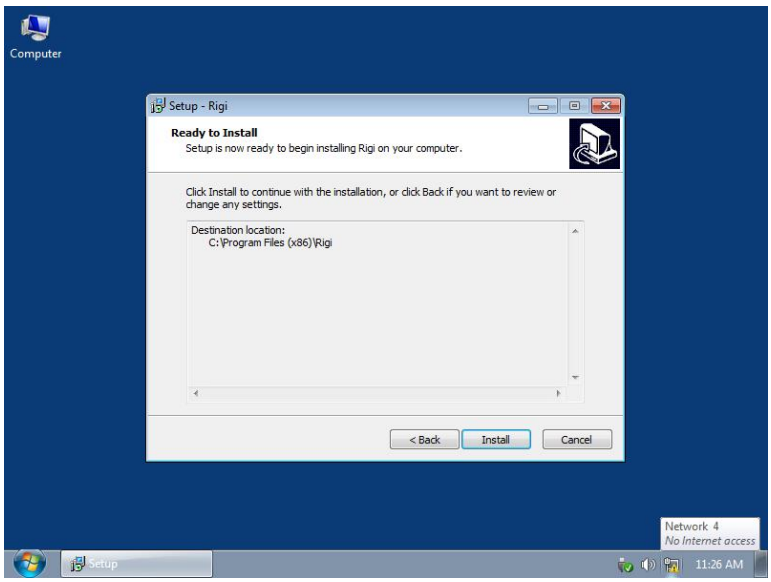
- Certificate Validation is not Applicable ?

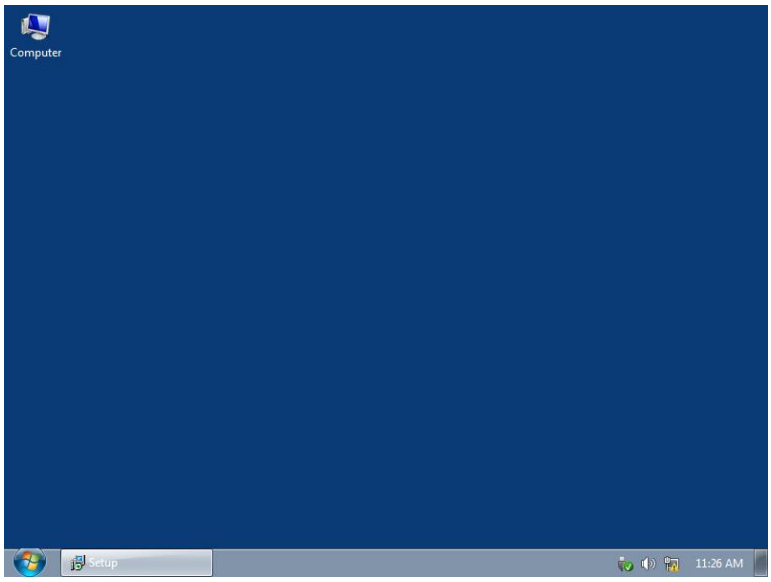
SCREENSHOTS




Computer
Setup - Rigi
Select Destination Location
Where should Rigi be installed?
Setup will install Rigi into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files (x86)\Rigi
Browse...
At least 0.8 MB of free disk space is required.
< Back
Next >
Cancel
Setup
11:26 AM

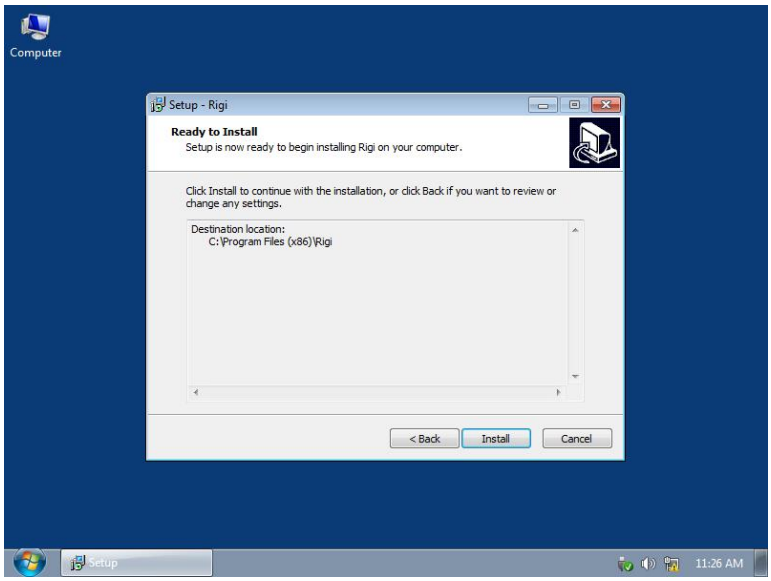

Computer
Setup - Rigi
Installing
Please wait while Setup installs Rigi on your computer.
Extracting files...
C:\Program Files (x86)\Rigi\Tatokerulon.pptx
Cancel
Setup
11:26 AM

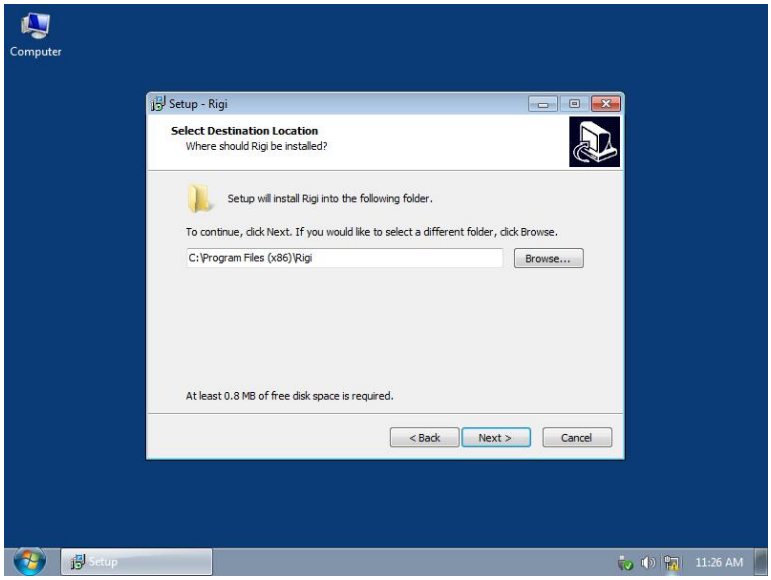

Computer
Setup - Rigi
Ready to Install
Setup is now ready to begin installing Rigi on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files (x86)\Rigi
< Back
Install
Cancel
Network 4
No Internet access
Setup
11:26 AM


Computer
Setup
11:26 AM


Computer
11:26 AM


Computer
11:27 AM


Computer
Setup - Rigi
Ready to Install
Setup is now ready to begin installing Rigi on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files (x86)\Rigi
< Back
Install
Cancel
Setup
11:26 AM


Computer
Setup - Rigi
Select Destination Location
Where should Rigi be installed?
Setup will install Rigi into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files (x86)\Rigi
Browse...
At least 0.8 MB of free disk space is required.
< Back
Next >
Cancel
Setup
11:26 AM