VALKYRIE COMODO

Summary

File Name: RIFZBJX.exe

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

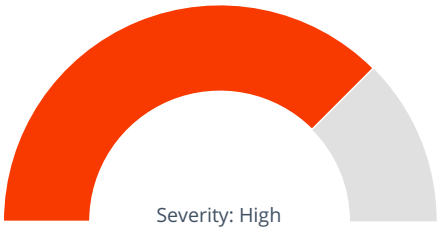
SHA1: 917b2f646ee7700f1e38d42a8810f67c9633c83a

MD5: ec46453ecc39a9798562226d5c580ff5

MALWARE

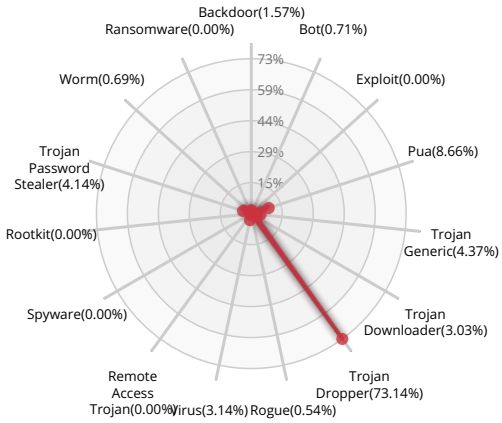
Valkyrie Final Verdict

DETECTION SECTION

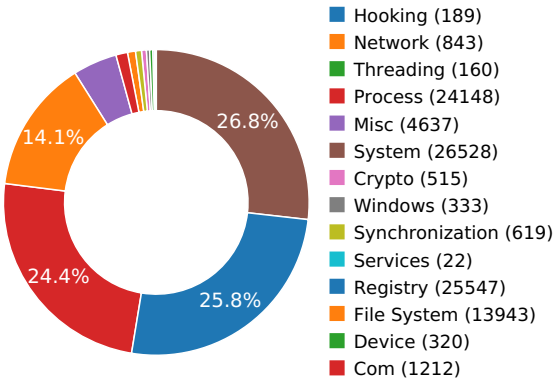


Verdict: Malware

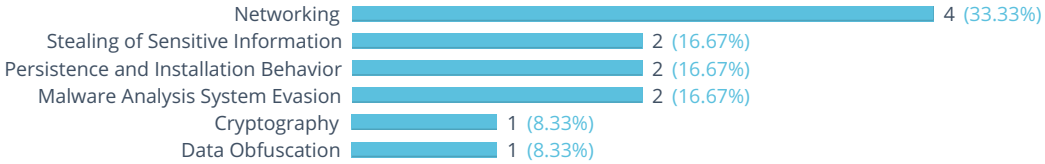
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

NETWORKING

Attempts to connect to a dead IP:Port (9 unique times)	Show sources
HTTP traffic contains suspicious features which may be indicative of malware related traffic	Show sources
Performs some HTTP requests	Show sources
Network activity contains more than one unique useragent.	Show sources

CRYPTOGRAPHY

At least one IP Address, Domain, or File Name was found in a crypto call	Show sources

STEALING OF SENSITIVE INFORMATION

Collects information to fingerprint the system	Show sources
Collects information about installed applications	Show sources

DATA OBFUSCATION

Drops a binary and executes it	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

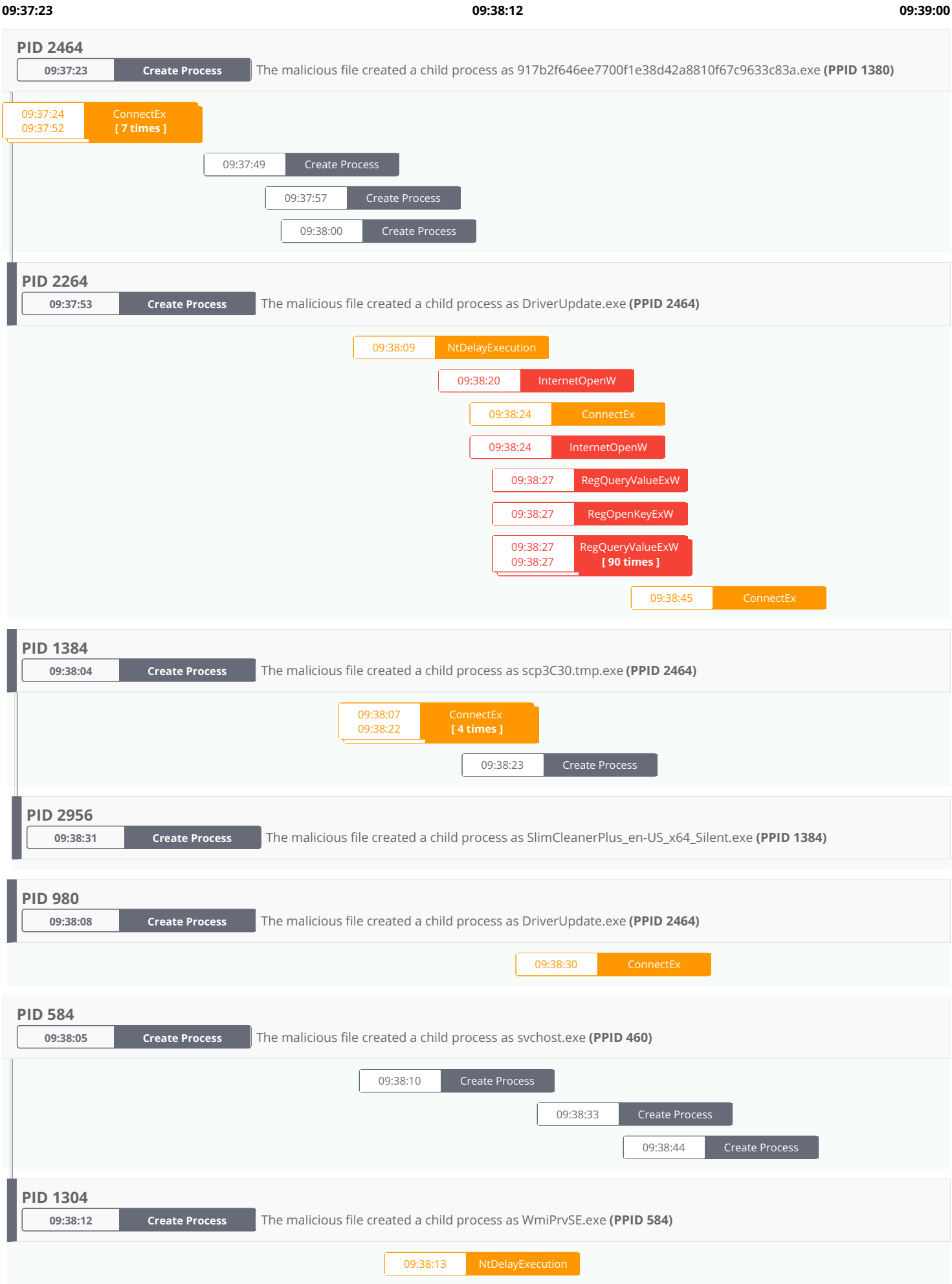
Installs itself for autorun at Windows startup	Show sources
Created a service that was not started	Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task.	Show sources
Detects VirtualBox through the presence of a registry key	Show sources

VALKYRIE COMODO

Behavior Graph



09:38:23	RegQueryValueExW

PID 2660

09:38:42	Create Process	The malicious file created a child process as unsecapp.exe **(PPID 584)**

PID 2740

09:38:54	Create Process	The malicious file created a child process as dllhost.exe **(PPID 584)**

PID 1760

09:38:12	Create Process	The malicious file created a child process as svchost.exe **(PPID 460)**

PID 872

09:39:00	Create Process	The malicious file created a child process as svchost.exe **(PPID 460)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES
C:\Users\user\AppData\Local\Temp\917b2f646ee7700f1e38d42a8810f67c9633c83a.exe.2.Manifest
C:\Users\user\AppData\Local\Temp\917b2f646ee7700f1e38d42a8810f67c9633c83a.exe.3.Manifest
C:\Users\user\AppData\Local\Temp\917b2f646ee7700f1e38d42a8810f67c9633c83a.exe.Config
C:\Users\user\AppData\Local\Temp\917b2f646ee7700f1e38d42a8810f67c9633c83a.exe
C:\Users\user\AppData\Local\Temp\917b2f646ee7700f1e38d42a8810f67c9633c83a.exe.1000.Manifest
C:\Users\user\AppData\Local\Temp\917b2f646ee7700f1e38d42a8810f67c9633c83aENU.dll
C:\Users\user\AppData\Local\Temp\917b2f646ee7700f1e38d42a8810f67c9633c83aLOC.dll
C:\Windows\Fonts\staticcache.dat
C:\Windows\win.ini
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\917b2f646ee7700f1e38d42a8810f67c9633c83a.exe.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\swu2B56.tmp
C:\
C:\Users\user\AppData\Local\Temp\swu2B56.tmp.msi
C:\Users\user\AppData\Local\Temp\scp3C30.tmp
C:\Users\user\AppData\Local\Temp\scp3C30.tmp.exe
C:\Users\Public\Documents\Downloaded Installers
C:\Users\Public\Documents\Downloaded Installers\{055C7DA5-A1F5-41FB-932C-82474ED3487A}
C:\Users\Public\Documents\Downloaded Installers\{055C7DA5-A1F5-41FB-932C-82474ED3487A}\setup.msi
C:\Users\user\AppData\Local\Temp\
A:
B:
F:
G:
H:
I:
J:
K:
L:

M:
N:
O:
P:
Q:
R:
S:
T:
U:
V:
W:
X:
Y:
Z:
C:\Users\user\AppData\Local\Temp\MSI4909.LOG
C:\Users\user\AppData\Local\Temp\MsiMsg.dll
C:\Windows\System32\msimsg.dll
C:\Windows\SysWOW64\shell32.dll
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate
C:\Program Files (x86)\DriverUpdate
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local\SlimWare Utilities Inc
C:
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\settings.db
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\settings.db-journal
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\settings.db-wal
\??\MountPointManager
C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe.2.Manifest
C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe.3.Manifest
C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe.Config
C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe

C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe.1000.Manifest
C:\Program Files (x86)\DriverUpdate\DriverUpdateENU.dll
C:\Program Files (x86)\DriverUpdate\DriverUpdateLOC.dll
C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe.Local\
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Logs
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Logs\2018-08-07 19-20-30 0.log
C:\ProgramData\Microsoft\Network\Connections\Pbk\rasphone.pbk

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\MachineID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\Registration\InstallationID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\Tracing\Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ShareCredsWithWinHttp
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\DisableBranchCache
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_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
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Miriam Transparent
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Fixed Miriam Transparent
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Rod Transparent
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\FangSong_GB2312
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\KaiTi_GB2312
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer\DisableUserInstalls
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer\Debug
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer\Timeout
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer\DisableLoggingFromPackage
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer\Logging

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\swu2B56.tmp
C:\Users\user\AppData\Local\Temp\swu2B56.tmp.msi
C:\Users\user\AppData\Local\Temp\scp3C30.tmp
C:\Users\user\AppData\Local\Temp\scp3C30.tmp.exe
C:\Users\Public\Documents\Downloaded Installers\{055C7DA5-A1F5-41FB-932C-82474ED3487A}\setup.msi
C:\Users\user\AppData\Local\Temp\MSI4909.LOG
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\settings.db
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\settings.db-journal
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Logs\2018-08-07 19-20-30 0.log
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\SWDUMon.inf
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\SWDUMon.sys
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\SWDUMon.cat
C:\Windows\inf\setupapi.app.log
C:\Windows\sysnative\drivers\SET81C7.tmp
C:\Windows\sysnative\drivers\SWDUMon.sys

C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\supdates.db
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\supdates.db-journal
C:\Windows\Tasks\DriverUpdate Scan.job
C:\Users\user\AppData\Local\Temp\TFR6BC5.tmp
C:\Windows\Tasks\DriverUpdate Startup.job
C:\Users\user\AppData\Local\Temp\TFR6D1E.tmp
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Images\acer.png
C:\Users\user\AppData\Local\Temp\SWIBD45.tmp
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\9A19ADAD9D098E039450ABBEDD5616EB_90968CAB679DC8A66D51322A089E7CBE
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\9A19ADAD9D098E039450ABBEDD5616EB_90968CAB679DC8A66D51322A089E7CBE
C:\Users\user\AppData\Local\Temp\SlimCleanerPlus_en-US_x64_Silent.exe
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Logs\2018-08-07 19-20-29 0.log
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM
\??\WMIDataDevice
\??\PIPE\lsarpc
\??\PIPE\srvsvc
\??\PIPE\wkssvc
C:\Users\user\AppData\Local\Temp\SIOUT35716500\SlimCleanerPlus_en-US_x64.msi
C:\Users\user\AppData\Local\Downloaded Installers\{7E03DFCF-3091-4D7A-91AB-59994A7A36B6}\setup.msi
C:\Users\user\AppData\Local\Temp\MSI1281e.LOG
C:\Windows\sysnative\Tasks\DriverUpdate Scan
C:\Windows\sysnative\Tasks\DriverUpdate Startup

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.FlsFree
kernel32.dll.InitializeCriticalSectionAndSpinCount
kernel32.dll.IsProcessorFeaturePresent
kernel32.dll.CreateActCtxW
kernel32.dll.ReleaseActCtx
kernel32.dll.ActivateActCtx
kernel32.dll.DeactivateActCtx
user32.dll.NotifyWinEvent

cryptbase.dll.SystemFunction036
user32.dll.GetWindowInfo
user32.dll.GetAncestor
user32.dll.GetMonitorInfoA
user32.dll.EnumDisplayMonitors
user32.dll.EnumDisplayDevicesA
gdi32.dll.ExtTextOutW
gdi32.dll.GdiIsMetaPrintDC
kernel32.dll.GetUserDefaultUILanguage
kernel32.dll.GetSystemDefaultUILanguage
kernel32.dll.FindActCtxSectionStringW
kernel32.dll.IsWow64Process
shlwapi.dll.StrRChrA
oleaut32.dll.#8
oleaut32.dll.#12
comctl32.dll.InitCommonControlsEx
dwmapi.dll.DwmIsCompositionEnabled
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
user32.dll.GetSystemMetrics
user32.dll.MonitorFromWindow
user32.dll.MonitorFromRect
user32.dll.MonitorFromPoint
user32.dll.EnumDisplayDevicesW
user32.dll.GetMonitorInfoW

ole32.dll.CoInitializeEx
ole32.dll.CoUninitialize
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoRevokeInitializeSpy
comctl32.dll.RegisterClassNameW
uxtheme.dll.EnableThemeDialogTexture
uxtheme.dll.OpenThemeData
uxtheme.dll.GetThemeBool
comctl32.dll.HIMAGELIST_QueryInterface
comctl32.dll.DrawShadowText
comctl32.dll.DrawSizeBox
comctl32.dll.DrawScrollBar
comctl32.dll.SizeBoxHwnd
comctl32.dll.ScrollBar_MouseMove
comctl32.dll.ScrollBar_Menu
comctl32.dll.HandleScrollCmd
comctl32.dll.DetachScrollBars
comctl32.dll.AttachScrollBars
comctl32.dll.CCSetScrollInfo
comctl32.dll.CCGetScrollInfo
comctl32.dll.CCEnableScrollBar
comctl32.dll.QuerySystemGestureStatus
uxtheme.dll.#49
uxtheme.dll.CloseThemeData
advapi32.dll.RegDeleteTreeA
advapi32.dll.RegDeleteTreeW
ole32.dll.CoTaskMemAlloc
ole32.dll.StringFromIID
nsi.dll.NsiAllocateAndGetTable
cfgmgr32.dll.CM_Open_Class_Key_ExW

DELETED FILES

C:\Users\user\AppData\Local\Temp\swu2B56.tmp
C:\Users\user\AppData\Local\Temp\swu2B56.tmp.msi
C:\Users\user\AppData\Local\Temp\scp3C30.tmp

C:\Users\user\AppData\Local\Temp\scp3C30.tmp.exe
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\settings.db-wal
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\settings.db-journal
C:\Windows\sysnative\drivers\SET81C7.tmp
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\supdates.db-wal
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\supdates.db-journal
C:\Users\user\AppData\Local\Temp\TFR6D1E.tmp
C:\Users\user\AppData\Local\Temp\SlimCleanerPlus_en-US_x64_Silent.exe
C:\Users\user\AppData\Local\Temp\SWIBD45.tmp

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\SlimWare Utilities Inc\DriverUpdate\InstallScanID
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\SWDUMon\WOW64

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en
HKEY_LOCAL_MACHINE\SOFTWARE\SlimWare Utilities Inc
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\Registration
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\MachineID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\Registration\InstallationID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\Tracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\Tracing\Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ShareCredsWithWinHttp
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\DisableBranchCache
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\917b2f646ee7700f1e38d42a8810f67c9633c83a.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
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\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
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

EXECUTED COMMANDS

"C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe" -installscan
"C:\Users\user\AppData\Local\Temp\scp3C30.tmp.exe" SI_LAUNCH=onreboot SI_MODE=toaster SI_DELAY=5 @P2_ORIGIN=^SW1^xdm111 @P2=^SW2^xdm229^^ @UL_STUBID=1425c179-ca0b-45a1-8652-62d33f76481c
"C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe" -installresults
"C:\Users\user\AppData\Local\Temp\SlimCleanerPlus_en-US_x64_Silent.exe" SI_LAUNCH=onreboot SI_MODE=toaster SI_DELAY=5
C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
C:\Windows\system32\wbem\unsecapp.exe -Embedding
C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}

READ FILES

C:\Users\user\AppData\Local\Temp\917b2f646ee7700f1e38d42a8810f67c9633c83a.exe.2.Manifest
C:\Users\user\AppData\Local\Temp\917b2f646ee7700f1e38d42a8810f67c9633c83a.exe.3.Manifest
C:\Users\user\AppData\Local\Temp\917b2f646ee7700f1e38d42a8810f67c9633c83a.exe.Config

C:\Users\user\AppData\Local\Temp\917b2f646ee7700f1e38d42a8810f67c9633c83a.exe
C:\Users\user\AppData\Local\Temp\917b2f646ee7700f1e38d42a8810f67c9633c83a.exe.1000.Manifest
C:\Windows\Fonts\staticcache.dat
C:\Windows\win.ini
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\swu2B56.tmp
C:\Users\user\AppData\Local\Temp\scp3C30.tmp
C:\Users\user\AppData\Local\Temp\swu2B56.tmp.msi
C:\Users\Public\Documents\Downloaded Installers\{055C7DA5-A1F5-41FB-932C-82474ED3487A}\setup.msi
C:\Windows\System32\msimsg.dll
C:\Windows\SysWOW64\shell32.dll
C:
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\settings.db
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\settings.db-journal
C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe.2.Manifest
C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe.3.Manifest
C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe.Config
C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe
C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe.1000.Manifest
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\ignores.dat
C:\Windows\System32\tzres.dll
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\SWDUMon.inf
C:\Windows\inf\setupapi.app.log
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\SWDUMon.sys
C:\Windows\sysnative\drivers\SET81C7.tmp
C:\Windows\inf\msmouse.inf
C:\Windows\inf\netrasa.inf
C:\Windows\inf\acpi.inf
C:\Windows\inf\umbus.inf
C:\Windows\inf\mshdc.inf
C:\Windows\inf\netsstpa.inf
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\rupdates.db
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\supdates.db

C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\supdates.db-journal
C:\Windows\inf\machine.inf
C:\Windows\inf\usbport.inf
C:\Windows\inf\rdpbus.inf
C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\oem16.CAT
C:\Windows\inf\oem16.inf
C:\Windows\inf\battery.inf
C:\Windows\inf\input.inf
C:\Windows\inf\monitor.inf
C:\Windows\inf\nete1g3e.inf
C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\oem15.CAT
C:\Windows\inf\oem15.inf
C:\Windows\inf\hdaudio.inf
C:\Windows\inf\volume.inf
C:\Windows\inf\cpu.inf
C:\Windows\inf\cdrom.inf
C:\Windows\inf\hdaudbus.inf
C:\Windows\inf\netavpna.inf
C:\Windows\inf\nettun.inf
C:\Windows\inf\hal.inf
C:\Windows\inf\keyboard.inf
C:\Windows\inf\blbdrive.inf
C:\Windows\inf\msports.inf
C:\Windows\inf\compositebus.inf
C:\Windows\inf\disk.inf
C:\Windows\System32\UxTheme.dll.Config
C:\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\COMCTL32.dll.mui
C:\Users\user\AppData\Local\Temp\TFR6BC5.tmp
C:\Users\user\AppData\Local\Temp\TFR6D1E.tmp
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\SWIBD45.tmp
C:\Windows\System32\p2pcollab.dll
C:\Windows\System32\en-US\DNSAPI.dll.mui
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115

MUTEXES

{042B0D65-EF5B-4E3F-ADFF-86C726E4F053}
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Global\MSILOG_1e1bf94b1d42e19GOL.9094ISM_pmeT_lacoL_ataDppA_resu_sresU_:C
Global_MSIExecute
SlimWare Utilities, Inc..DriverUpdate
IESQMMUTEX_0_208
Global\MSILOG_4991c73e1d42e19GOL.e1821ISM_pmeT_lacoL_ataDppA_resu_sresU_:C

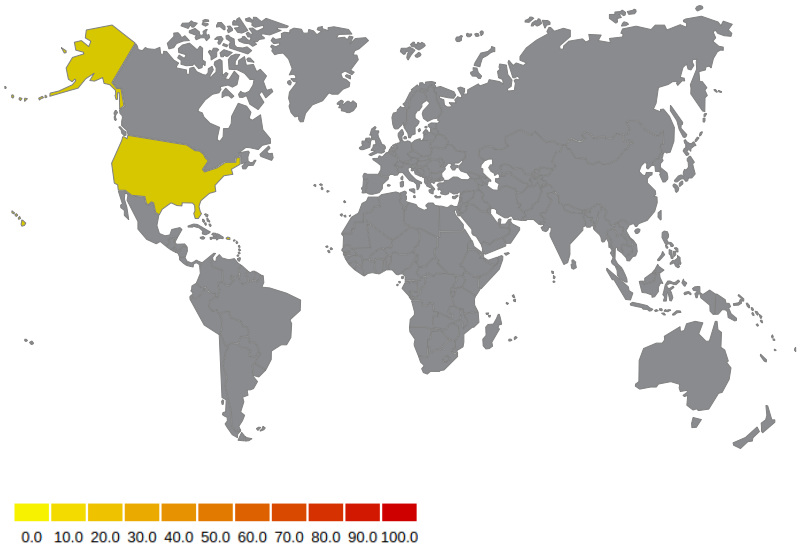
MODIFIED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\SlimWare Utilities Inc
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\Registration
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\MachineID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\GlobalAssocChangedCounter
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\tbInstallationSessionID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\InstallationSessionID
HKEY_CURRENT_USER\SOFTWARE\SlimWare Utilities Inc\DriverUpdate
HKEY_CURRENT_USER\Software\SlimWare Utilities Inc\DriverUpdate\InstallationSessionID
HKEY_CURRENT_USER\Software\SlimWare Utilities Inc\tbInstallationSessionID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\InstallerData
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\InstallerData\browser
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\InstallerData\track
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\InstallerData\upl
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\Registration\InstallationID
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason

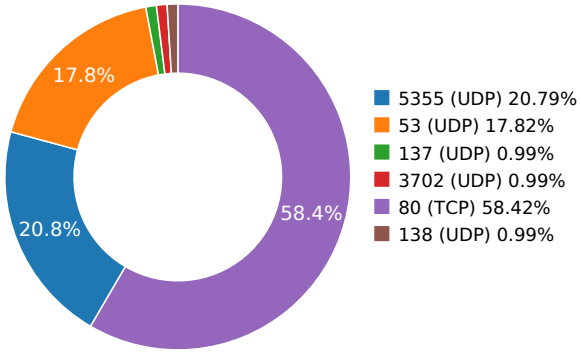
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\SlimWare Utilities Inc\DriverUpdate\InstallScanUrlParams
HKEY_LOCAL_MACHINE\SYSTEM\Setup\SetupapiLogStatus
HKEY_LOCAL_MACHINE\SYSTEM\Setup\SetupapiLogStatus\setupapi.app.log
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6E\52C64B7E\LanguageList
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\SWDUMon\BasePath
HKEY_LOCAL_MACHINE\SOFTWARE\SlimWare Utilities, Inc.\DriverApp\Installed
HKEY_LOCAL_MACHINE\SOFTWARE\SlimWare Utilities, Inc.\DriverApp\Downloaded
HKEY_CURRENT_USER\Software\SlimWare Utilities Inc\DriverUpdate\InstallScanID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\SlimCleaner Plus\Registration
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6E\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6E\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\SlimCleaner Plus\InstallerData
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\SlimCleaner Plus\InstallerData\p2
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\SlimCleaner Plus\InstallerData\secondOfferOrigin
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\SlimCleaner Plus\InstallerData\ul_stubid
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\SlimCleaner Plus\InstallerData\ul_track
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\SlimCleaner Plus\Registration\InstallationID
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_LOCAL_MACHINE\SOFTWARE\SlimWare Utilities Inc\DriverUpdate\PNGS
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\PNGS\RN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\DriverUpdate Scan.job
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\DriverUpdate Scan.job.fp
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{EE75A823-2DBB-4D9C-B247-336850C2B8D6}\Path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{EE75A823-2DBB-4D9C-B247-336850C2B8D6}\Hash
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\DriverUpdate Startup\Id
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\DriverUpdate Startup\Index
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{EE75A823-2DBB-4D9C-B247-336850C2B8D6}\Triggers
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{EE75A823-2DBB-4D9C-B247-336850C2B8D6}\DynamicInfo
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\DriverUpdate Startup.job
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\DriverUpdate Startup.job.fp

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	151.101.2.133	United States	54113	Fastly	Malware Process
	184.24.97.174	United States	20940	Akamai Technologies, Inc.	OS Process
	184.26.44.98	United States	20940	Akamai Technologies, Inc.	OS Process
	23.52.91.27	United States	1299	Akamai Technologies, Inc.	Malware Process
	52.216.128.186	United States	16509	Amazon Technologies Inc.	Malware Process
	52.216.169.26	United States	16509	Amazon Technologies Inc.	Malware Process
	52.54.9.186	United States	14618	Amazon Technologies Inc.	Malware Process
	52.55.74.238	United States	14618	Amazon Technologies Inc.	Malware Process
	52.6.81.132	United States	14618	Amazon Technologies Inc.	Malware Process
	52.85.98.74	United States	16509	Amazon Technologies Inc.	Malware Process
	52.85.98.87	United States	16509	Amazon Technologies Inc.	Malware Process
	54.84.213.244	United States	14618	Amazon Technologies Inc.	Malware Process
trk.slimwareutilities.com	54.175.217.102	United States	14618	Amazon Technologies Inc.	Malware Process
crl.globalsign.net	151.101.118.133	United States	54113	Fastly	Malware Process
cdn.slimcleaner.com	52.84.31.11	United States	16509	Amazon Technologies Inc.	Malware Process
driverrpc.slimwareutilities.com	54.82.77.150	United States	14618	Amazon Technologies Inc.	Malware Process
ocsp.verisign.com	23.50.75.27	United States	3257	Akamai Technologies, Inc.	Malware Process
apps-api.slimwareutilities.com	52.2.26.10	United States	14618	Amazon Technologies Inc.	Malware Process
crl.microsoft.com	209.48.71.155	United States	2828	MCI Communications Servic...	OS Process
ctldl.windowsupdate.com	209.48.71.144	United States	2828	MCI Communications Servic...	OS Process
sf.symcd.com	23.52.155.27	United States	1299	Akamai Technologies, Inc.	Malware Process
stats.slimwareutilities.com	52.216.17.170	United States	16509	Amazon Technologies Inc.	Malware Process

Name	IP	Country	ASN	ASN Name	Trigger Process Type
stc.slimwareutilities.com	54.209.147.46	United States	14618	Amazon Technologies Inc.	Malware Process
download.driverupdate.net	52.84.31.98	United States	16509	Amazon Technologies Inc.	Malware Process
www.driverupdate.net	52.54.197.47	United States	14618	Amazon Technologies Inc.	Malware Process
www.slimwareutilities.com	50.17.223.81	United States	14618	Amazon.com, Inc.	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
www.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	6.42169499397
Path: /installer/init_v2.php **URI:** http://www.slimwareutilities.com/installer/init_v2.php						
stats.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	7.90121912956
Path: /api/flow/action **URI:** http://stats.slimwareutilities.com/api/flow/action						
stats.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	7.92766904831
Path: /api/flow/action **URI:** http://stats.slimwareutilities.com/api/flow/action						
stats.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	7.94653296471
Path: /api/flow/action **URI:** http://stats.slimwareutilities.com/api/flow/action						
stats.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	7.96431708336
Path: /api/flow/action **URI:** http://stats.slimwareutilities.com/api/flow/action						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	8.97313594818
Path: /ulc.php? ev=InstallerInvoked&upl=YTo1OntzOjk6InVsX3N0dWJpZCI7czozNjoiMTQyNWMxNzktY2EwYi00NWExLTg2NTItNjJkMzNmNzY0ODFjIjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMjI5IjtzOjg6InVsX3N1YmlkIjtzOjI2OiJDTFgzMHRhUnlzc0NGUTF2dkFvZHVuTUVqQSI7czo3OiJwcm9kdWN0IjtzOjM6IlNXMiI7fQ%3D%3D&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F **URI:** http://trk.slimwareutilities.com/ulc.php? ev=InstallerInvoked&upl=YTo1OntzOjk6InVsX3N0dWJpZCI7czozNjoiMTQyNWMxNzktY2EwYi00NWExLTg2NTItNjJkMzNmNzY0ODFjIjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMjI5IjtzOjg6InVsX3N1YmlkIjtzOjI2OiJDTFgzMHRhUnlzc0NGUTF2dkFvZHVuTUVqQSI7czo3OiJwcm9kdWN0IjtzOjM6IlNXMiI7fQ%3D%3D&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F						
download.driverupdate.net	80	GET	1.1	SLIMHTTP/1.1	1	9.00639605522
Path: /DriverUpdate-setup.msi.bz2 **URI:** http://download.driverupdate.net/DriverUpdate-setup.msi.bz2						
stats.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	10.0572350025
Path: /api/flow/action **URI:** http://stats.slimwareutilities.com/api/flow/action						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	10.5410950184

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /ulc.php? ev=InstallerAccepted&upl=YTo1OntzOjk6InVsX3N0dWJpZCI7czozNjoiMTQyNWMxNzktY2EwYi00NWExLTg2NTItNjJkMzNmNzY0ODFjIjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMjI5IjtzOjg6InVsX3N1YmlkIjtzOjI2OiJDTFgzMHRhUnlzc0NGUTF2dkFvZHVuTUVqQSI7czo3OiJwcm9kdWN0IjtzOjM6IlNXMiI7fQ%3D%3D&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F **URI:** http://trk.slimwareutilities.com/ulc.php? ev=InstallerAccepted&upl=YTo1OntzOjk6InVsX3N0dWJpZCI7czozNjoiMTQyNWMxNzktY2EwYi00NWExLTg2NTItNjJkMzNmNzY0ODFjIjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMjI5IjtzOjg6InVsX3N1YmlkIjtzOjI2OiJDTFgzMHRhUnlzc0NGUTF2dkFvZHVuTUVqQSI7czo3OiJwcm9kdWN0IjtzOjM6IlNXMiI7fQ%3D%3D&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F						
cdn.slimcleaner.com	80	GET	1.1	SLIMHTTP/1.1	1	13.2645010948
Path: /downloads/scplus/SlimCleanerPlus.x64.Downloader.exe.bz2 **URI:** http://cdn.slimcleaner.com/downloads/scplus/SlimCleanerPlus.x64.Downloader.exe.bz2						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	19.7892560959
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?0a08099fe9039bd3 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?0a08099fe9039bd3						
ocsp.verisign.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	25.0848040581
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBS56bKHAoUD%2BOyl%2B0LhPg9JxyQm4gQUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMCEFIA5aolVvwahu2WydRLM8c%3D **URI:** http://ocsp.verisign.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBS56bKHAoUD%2BOyl%2B0LhPg9JxyQm4gQUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMCEFIA5aolVvwahu2WydRLM8c%3D						
sf.symcd.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	30.4058890343
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTSqZMG5M8TA9rdzkbCnNwuMAd5VgQUz5mp6nsm9EvJjo%2FX8AUm7%2BPSp50CECRrvoErNsE3IlSXuo3xePo%3D **URI:** http://sf.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTSqZMG5M8TA9rdzkbCnNwuMAd5VgQUz5mp6nsm9EvJjo%2FX8AUm7%2BPSp50CECRrvoErNsE3IlSXuo3xePo%3D						
stats.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	32.0320911407
Path: /api/flow/action **URI:** http://stats.slimwareutilities.com/api/flow/action						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	34.5125801563
Path: /ulc.php? ev=InstallerFinished&upl=YTo1OntzOjk6InVsX3N0dWJpZCI7czozNjoiMTQyNWMxNzktY2EwYi00NWExLTg2NTItNjJkMzNmNzY0ODFjIjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMjI5IjtzOjg6InVsX3N1YmlkIjtzOjI2OiJDTFgzMHRhUnlzc0NGUTF2dkFvZHVuTUVqQSI7czo3OiJwcm9kdWN0IjtzOjM6IlNXMiI7fQ%3D%3D&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F&installId=20C72032-4E71-4681-A2F0-22ADEFB7F62B **URI:** http://trk.slimwareutilities.com/ulc.php? ev=InstallerFinished&upl=YTo1OntzOjk6InVsX3N0dWJpZCI7czozNjoiMTQyNWMxNzktY2EwYi00NWExLTg2NTItNjJkMzNmNzY0ODFjIjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMjI5IjtzOjg6InVsX3N1YmlkIjtzOjI2OiJDTFgzMHRhUnlzc0NGUTF2dkFvZHVuTUVqQSI7czo3OiJwcm9kdWN0IjtzOjM6IlNXMiI7fQ%3D%3D&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F&installId=20C72032-4E71-4681-A2F0-22ADEFB7F62B						
stats.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	40.2601139545
Path: /api/flow/action **URI:** http://stats.slimwareutilities.com/api/flow/action						
stats.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	43.0376520157
Path: /api/flow/action **URI:** http://stats.slimwareutilities.com/api/flow/action						
stc.slimwareutilities.com	80	GET	1.1	SilentDownloader/2.4.1	1	43.5261049271
Path: /gettrack?product=SW1&p2=%5ESW2%5Exdm229%5E%5E&secondOfferOrigin=%5ESW1%5Exdm111&ul_stubid=1425c179-ca0b-45a1-8652-62d33f76481c **URI:** http://stc.slimwareutilities.com/gettrack?product=SW1&p2=%5ESW2%5Exdm229%5E%5E&secondOfferOrigin=%5ESW1%5Exdm111&ul_stubid=1425c179-ca0b-45a1-8652-62d33f76481c						
cdn.slimcleaner.com	80	GET	1.1	SilentDownloader/2.4.1	1	43.765360117

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /downloads/scplus/SlimCleanerPlus_en-US_x64_Silent.exe **URI:** http://cdn.slimcleaner.com/downloads/scplus/SlimCleanerPlus_en-US_x64_Silent.exe						
trk.slimwareutilities.com	80	GET	1.1	SilentDownloader/2.4.1	1	43.7734191418
Path: /ulc.php?ev=InstallerInvoked&platformOSVersion=6.1&secondOfferOrigin=%5ESW1%5Exdm111&ul_stubid=1425c179-ca0b-45a1-8652-62d33f76481c&p2=%5ESW2%5Exdm229%5E%5E&installer=SD0&product=SW1&installerVersion=2.4.1&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F&platformOS=Windows&ul_track=SCP077 **URI:** http://trk.slimwareutilities.com/ulc.php?ev=InstallerInvoked&platformOSVersion=6.1&secondOfferOrigin=%5ESW1%5Exdm111&ul_stubid=1425c179-ca0b-45a1-8652-62d33f76481c&p2=%5ESW2%5Exdm229%5E%5E&installer=SD0&product=SW1&installerVersion=2.4.1&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F&platformOS=Windows&ul_track=SCP077						
sf.symcd.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	58.8412139416
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTSqZMG5M8TA9rdzkbCnNwuMAd5VgQUz5mp6nsm9EvJjo%2FX8AUm7%2BPSp50CEDBjs6dAwc39%2BLuebDMa194%3D **URI:** http://sf.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTSqZMG5M8TA9rdzkbCnNwuMAd5VgQUz5mp6nsm9EvJjo%2FX8AUm7%2BPSp50CEDBjs6dAwc39%2BLuebDMa194%3D						
apps-api.slimwareutilities.com	80	POST	1.1	PHP.Serialize	2	61.9651761055
Path: /v1/AutoActivate **URI:** http://apps-api.slimwareutilities.com/v1/AutoActivate						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	62.6414029598
Path: /ulc.php?ev=Startup&installId=20C72032-4E71-4681-A2F0-22ADEFB7F62B&browser=chrome&productVersion=2.7.11.0&product=SW2&hasUI=no&upl=YTo1OntzOjk6InVsX3N0dWJpZCI7czozNjoiMTQyNWMxNzktY2EwYi00NWExLTg2NTItNjJkMzNmNzY0ODFjIjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMjI5IjtzOjg6InVsX3N1YmlkIjtzOjI2OiJDTFgzMHRhUnlzc0NGUTF2dkFvZHVuTUVqQSI7czo3OiJwcm9kdWN0IjtzOjM6IlNXMiI7fQ%3D%3D&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F&isRegistered=no&eventSource=SYSTEM **URI:** http://trk.slimwareutilities.com/ulc.php?ev=Startup&installId=20C72032-4E71-4681-A2F0-22ADEFB7F62B&browser=chrome&productVersion=2.7.11.0&product=SW2&hasUI=no&upl=YTo1OntzOjk6InVsX3N0dWJpZCI7czozNjoiMTQyNWMxNzktY2EwYi00NWExLTg2NTItNjJkMzNmNzY0ODFjIjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMjI5IjtzOjg6InVsX3N1YmlkIjtzOjI2OiJDTFgzMHRhUnlzc0NGUTF2dkFvZHVuTUVqQSI7czo3OiJwcm9kdWN0IjtzOjM6IlNXMiI7fQ%3D%3D&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F&isRegistered=no&eventSource=SYSTEM						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	62.7860119343
Path: /pki/crl/products/tspca.crl **URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl						
www.slimwareutilities.com	80	GET	1.1	DriverUpdate	1	62.8542749882
Path: /download_stats/new_install.php?program=DriverUpdate2 **URI:** http://www.slimwareutilities.com/download_stats/new_install.php?program=DriverUpdate2						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	63.1544790268
Path: /pki/crl/products/CodeSignPCA2.crl **URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	63.36028409
Path: /pki/crl/products/WinPCA.crl **URI:** http://crl.microsoft.com/pki/crl/products/WinPCA.crl						
crl.globalsign.net	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	63.5777759552
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	65.1198530197

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /ulc.php?ev=Startup&installId=20C72032-4E71-4681-A2F0-22ADEFB7F62B&browser=chrome&productVersion=2.7.11.0&product=SW2&hasUI=yes&upl=YTo1OntzOjk6InVsX3N0dWJpZCI7czozNjoiMTQyNWMxNzktY2EwYi00NWExLTg2NTItNjJkMzNmNzY0ODFjIjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMjI5IjtzOjg6InVsX3N1YmlkIjtzOjI2OiJDTFgzMHRhUnlzc0NGUTF2dkFvZHVuTUVqQSI7czo3OiJwcm9kdWN0IjtzOjM6IlNXMiI7fQ%3D%3D&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F&isRegistered=no&eventSource=SYSTEM **URI:** http://trk.slimwareutilities.com/ulc.php?ev=Startup&installId=20C72032-4E71-4681-A2F0-22ADEFB7F62B&browser=chrome&productVersion=2.7.11.0&product=SW2&hasUI=yes&upl=YTo1OntzOjk6InVsX3N0dWJpZCI7czozNjoiMTQyNWMxNzktY2EwYi00NWExLTg2NTItNjJkMzNmNzY0ODFjIjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMjI5IjtzOjg6InVsX3N1YmlkIjtzOjI2OiJDTFgzMHRhUnlzc0NGUTF2dkFvZHVuTUVqQSI7czo3OiJwcm9kdWN0IjtzOjM6IlNXMiI7fQ%3D%3D&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F&isRegistered=no&eventSource=SYSTEM						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	84.1615581512
Path: /ulc.php?ev=UIView&installId=20C72032-4E71-4681-A2F0-22ADEFB7F62B&view=%2FMain%2FHome&browser=chrome&productVersion=2.7.11.0&product=SW2&sessionid=7D07B9B6-9E77-47C1-ADEC-E95F9CE3443C&upl=YTo1OntzOjk6InVsX3N0dWJpZCI7czozNjoiMTQyNWMxNzktY2EwYi00NWExLTg2NTItNjJkMzNmNzY0ODFjIjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMjI5IjtzOjg6InVsX3N1YmlkIjtzOjI2OiJDTFgzMHRhUnlzc0NGUTF2dkFvZHVuTUVqQSI7czo3OiJwcm9kdWN0IjtzOjM6IlNXMiI7fQ%3D%3D&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F **URI:** http://trk.slimwareutilities.com/ulc.php?ev=UIView&installId=20C72032-4E71-4681-A2F0-22ADEFB7F62B&view=%2FMain%2FHome&browser=chrome&productVersion=2.7.11.0&product=SW2&sessionid=7D07B9B6-9E77-47C1-ADEC-E95F9CE3443C&upl=YTo1OntzOjk6InVsX3N0dWJpZCI7czozNjoiMTQyNWMxNzktY2EwYi00NWExLTg2NTItNjJkMzNmNzY0ODFjIjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMjI5IjtzOjg6InVsX3N1YmlkIjtzOjI2OiJDTFgzMHRhUnlzc0NGUTF2dkFvZHVuTUVqQSI7czo3OiJwcm9kdWN0IjtzOjM6IlNXMiI7fQ%3D%3D&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F						
trk.slimwareutilities.com	80	GET	1.1	SilentDownloader/2.4.1	1	84.6575059891
Path: /ulc.php?ev=InstallerFinished&platformOSVersion=6.1&secondOfferOrigin=%5ESW1%5Exdm111&installId=98F229B8-37A6-4834-9675-83A2E55C6029&ul_stubid=1425c179-ca0b-45a1-8652-62d33f76481c&p2=%5ESW2%5Exdm229%5E%5E&installer=SD0&product=SW1&installerVersion=2.4.1&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F&platformOS=Windows&ul_track=SCP077 **URI:** http://trk.slimwareutilities.com/ulc.php?ev=InstallerFinished&platformOSVersion=6.1&secondOfferOrigin=%5ESW1%5Exdm111&installId=98F229B8-37A6-4834-9675-83A2E55C6029&ul_stubid=1425c179-ca0b-45a1-8652-62d33f76481c&p2=%5ESW2%5Exdm229%5E%5E&installer=SD0&product=SW1&installerVersion=2.4.1&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F&platformOS=Windows&ul_track=SCP077						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	88.5545930862
Path: /ulc.php?ev=UIView&installId=20C72032-4E71-4681-A2F0-22ADEFB7F62B&view=%2FIntro&browser=chrome&productVersion=2.7.11.0&product=SW2&sessionid=7D07B9B6-9E77-47C1-ADEC-E95F9CE3443C&upl=YTo1OntzOjk6InVsX3N0dWJpZCI7czozNjoiMTQyNWMxNzktY2EwYi00NWExLTg2NTItNjJkMzNmNzY0ODFjIjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMjI5IjtzOjg6InVsX3N1YmlkIjtzOjI2OiJDTFgzMHRhUnlzc0NGUTF2dkFvZHVuTUVqQSI7czo3OiJwcm9kdWN0IjtzOjM6IlNXMiI7fQ%3D%3D&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F **URI:** http://trk.slimwareutilities.com/ulc.php?ev=UIView&installId=20C72032-4E71-4681-A2F0-22ADEFB7F62B&view=%2FIntro&browser=chrome&productVersion=2.7.11.0&product=SW2&sessionid=7D07B9B6-9E77-47C1-ADEC-E95F9CE3443C&upl=YTo1OntzOjk6InVsX3N0dWJpZCI7czozNjoiMTQyNWMxNzktY2EwYi00NWExLTg2NTItNjJkMzNmNzY0ODFjIjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMjI5IjtzOjg6InVsX3N1YmlkIjtzOjI2OiJDTFgzMHRhUnlzc0NGUTF2dkFvZHVuTUVqQSI7czo3OiJwcm9kdWN0IjtzOjM6IlNXMiI7fQ%3D%3D&machineId=26A6A5CC-ED2C-4D1B-98D9-89F660C3BB1F						
driverrpc.slimwareutilities.com	80	POST	1.1	HTTPPostLib/1.0	1	89.1449830532
Path: / **URI:** http://driverrpc.slimwareutilities.com/						
www.driverupdate.net	80	GET	1.1	DriverUpdate	1	89.6315591335
Path: /services/get_pc_brand.php?id=1 **URI:** http://www.driverupdate.net/services/get_pc_brand.php?id=1						
www.driverupdate.net	80	GET	1.1	DriverUpdate	1	89.6869001389
Path: /images/test/acer.png **URI:** http://www.driverupdate.net/images/test/acer.png						

DNS QUERIES

Request	Type
www.slimwareutilities.com	A

Request	Type
Answers - slimwareutilities.com (CNAME) - 50.17.223.81 (A)	
stats.slimwareutilities.com	A
Answers - 52.216.169.26 (A) - 52.216.128.186 (A)	
trk.slimwareutilities.com	A
Answers - trk-slimwareutilities-com-ms-270141606.us-east-1.elb.amazonaws.com (CNAME) - 34.231.33.210 (A) - 52.54.9.186 (A) - 54.175.217.102 (A)	
download.driverupdate.net	A
Answers - 52.85.98.87 (A) - 52.85.98.81 (A) - 52.85.98.169 (A) - 52.85.98.56 (A)	
cdn.slimcleaner.com	A
Answers - 52.85.98.129 (A) - 52.85.98.74 (A) - 52.85.98.34 (A) - 52.85.98.178 (A)	
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 184.24.97.176 (A) - a1621.g.akamai.net (CNAME) - ctldl.windowsupdate.com.edgesuite.net (CNAME) - 184.24.97.174 (A)	
ocsp.verisign.com	A
Answers - ocsp-ds.ws.symantec.com.edgekey.net (CNAME) - e8218.dscb1.akamaiedge.net (CNAME) - 23.52.91.27 (A)	
sf.symcd.com	A
stc.slimwareutilities.com	A
Answers - 54.209.147.46 (A) - stc-slimwareutilities-com-ms-1989010110.us-east-1.elb.amazonaws.com (CNAME) - 52.55.74.238 (A) - 52.20.7.33 (A)	
apps-api.slimwareutilities.com	A

Request	Type
Answers - apps-api-slimwareutilities-com-956522425.us-east-1.elb.amazonaws.com (CNAME) - 52.2.26.10 (A) - 52.44.174.33 (A) - 52.6.81.132 (A)	
crl.microsoft.com	A
Answers - 184.26.44.97 (A) - 184.26.44.98 (A) - crl.www.ms.akadns.net (CNAME) - a1363.dscg.akamai.net (CNAME)	
crl.globalsign.net	A
Answers - 151.101.66.133 (A) - 151.101.2.133 (A) - global.prd.cdn.globalsign.com (CNAME) - 151.101.194.133 (A) - 151.101.130.133 (A) - prod.globalsign.map.fastly.net (CNAME)	
driverrpc.slimwareutilities.com	A
Answers - 54.82.77.150 (A)	
www.driverupdate.net	A
Answers - 54.84.213.244 (A) - 34.226.146.234 (A) - 52.54.197.47 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.42169499397	Sandbox	50.17.223.81	80
7.90121912956	Sandbox	52.216.169.26	80
8.97313594818	Sandbox	52.54.9.186	80
9.00639605522	Sandbox	52.85.98.87	80
13.2645010948	Sandbox	52.85.98.74	80
19.7892560959	Sandbox	184.24.97.174	80
25.0848040581	Sandbox	23.52.91.27	80
30.4058890343	Sandbox	23.52.91.27	80
32.0320911407	Sandbox	52.216.128.186	80
34.5125801563	Sandbox	52.54.9.186	80
43.5261049271	Sandbox	52.55.74.238	80
43.765360117	Sandbox	52.85.98.74	80
43.7734191418	Sandbox	52.54.9.186	80
58.8412139416	Sandbox	23.52.91.27	80
61.9651761055	Sandbox	52.6.81.132	80
62.2611629963	Sandbox	52.6.81.132	80
62.6414029598	Sandbox	52.54.9.186	80
62.7860119343	Sandbox	184.26.44.98	80
62.8542749882	Sandbox	50.17.223.81	80
63.5777759552	Sandbox	151.101.2.133	80
65.1198530197	Sandbox	52.54.9.186	80
84.1615581512	Sandbox	54.175.217.102	80
89.1449830532	Sandbox	54.82.77.150	80
89.6315591335	Sandbox	54.84.213.244	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.21490502357	Sandbox	224.0.0.252	5355
3.22679209709	Sandbox	192.168.56.255	137
3.237885952	Sandbox	224.0.0.252	5355
3.27067613602	Sandbox	239.255.255.250	3702
5.81349802017	Sandbox	224.0.0.252	5355
6.2187230587	Sandbox	192.168.56.255	138
6.34173107147	Sandbox	224.0.0.252	5355
6.34281611443	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.37437009811	Sandbox	224.0.0.252	5355
7.84235906601	Sandbox	8.8.4.4	53
7.9238409996	Sandbox	224.0.0.252	5355
8.90165495872	Sandbox	8.8.4.4	53
8.95131397247	Sandbox	8.8.4.4	53
10.6616630554	Sandbox	224.0.0.252	5355
13.2135679722	Sandbox	8.8.4.4	53
14.4854569435	Sandbox	224.0.0.252	5355
17.072124958	Sandbox	224.0.0.252	5355
19.6376149654	Sandbox	8.8.4.4	53
19.8896460533	Sandbox	224.0.0.252	5355
22.4719769955	Sandbox	224.0.0.252	5355
25.0345749855	Sandbox	8.8.4.4	53
25.1225280762	Sandbox	224.0.0.252	5355
27.6948621273	Sandbox	224.0.0.252	5355
30.2447850704	Sandbox	8.8.4.4	53
30.2839429379	Sandbox	8.8.4.4	53
31.905105114	Sandbox	8.8.4.4	53
31.9147839546	Sandbox	224.0.0.252	5355
40.5947999954	Sandbox	224.0.0.252	5355
43.366740942	Sandbox	8.8.4.4	53
53.1505379677	Sandbox	224.0.0.252	5355
55.9621560574	Sandbox	224.0.0.252	5355
58.7854650021	Sandbox	8.8.4.4	53
58.8230140209	Sandbox	224.0.0.252	5355
59.2902650833	Sandbox	224.0.0.252	5355
59.9152340889	Sandbox	224.0.0.252	5355
61.8541679382	Sandbox	8.8.4.4	53
62.3846020699	Sandbox	224.0.0.252	5355
62.7310781479	Sandbox	8.8.4.4	53
63.5318031311	Sandbox	8.8.4.4	53
84.1198890209	Sandbox	8.8.4.4	53
89.0838589668	Sandbox	8.8.4.4	53
89.5915560722	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Supdates.Db-Journal	**Type :** data **MD5 :** 20c532bdb8e4e2dd3076f8f1629cf54e **SHA-1 :** e61f611b39e779975f34a805de9db6616038ccea **SHA-256 :** 8ce0ab36d1e16b989baae3d11364cadf9872959 **SHA-512 :** d87a6f7e1c125e03ade1e090b266b0af1f204ff07 **Size :** 1.544 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 748ba8fd669c95bd464e7a75aff23dfb **SHA-1 :** 6807fcde1c619e2a48d037e19107b6a28af280c3 **SHA-256 :** 4d10f0959cf070aab46740a72f19f9e038244df82 **SHA-512 :** c3938ec688300be32ac74d689a4b6bd916b5bd3 **Size :** 5.672 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 406a41faf0c34983b66025eabc9c16e8 **SHA-1 :** 7261ad36d62e7fd58224ff8437f8b44c0b933a6a **SHA-256 :** 7d3edf2b9333bbde89bc48d54538afeb4dca82fc **SHA-512 :** e6e678b6cd9c92294c64caab84478de60f7c5ff73 **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\Temp\Scp3C30.Tmp.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 5d3bd16be3d9e0ae2e14c90c3887cb4b **SHA-1 :** dbc097bf3a56d2cea3ac91b2085c12bb64eebe50 **SHA-256 :** b9a7d055586a04ec261416c2f1c2368d22dffbc0f **SHA-512 :** da75edf51b09ecc744eb6284265755662baaac3c **Size :** 253.016 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** fbd21c2a4a7bb541b10d48cb1b693880 **SHA-1 :** 0d69e698f1b23d67b38f533da9fc0e010d32c78e **SHA-256 :** 8f0fcb207ae50ca9ee0410dfc4614c81667b73b81 **SHA-512 :** c53fec5515ef5e53adfeaefbb28d59b8128dd75d7 **Size :** 1.544 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Supdates.Db-Journal	**Type :** data **MD5 :** f4adc01cd83fa02615ce95915936a368 **SHA-1 :** 830d5366285908f87a66786cb10e5061db0837a6 **SHA-256 :** fe297c458679899a34cf196b42d49f94bcae9ce67 **SHA-512 :** 1c9c97e5a398f5f7ae724c0b1202263f036aac3bf **Size :** 1.544 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 1dfa827c5394f4c4839dfed80ede2aa7 **SHA-1 :** c41a2d725d5d4ff1157ee89e86f5879e088e4db0 **SHA-256 :** 12e754f5abebc8c7ac26389104cf28e604779a958 **SHA-512 :** 594c2518ad0cda75ffb76d489edf0cf748657964a **Size :** 2.576 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Logs\2018-08-07 19-20-30 0.Log	**Type :** ASCII text, with CRLF line terminators **MD5 :** e0d813989f241bafd5057ff1c259583d **SHA-1 :** 1ada81489cfc249d05ef34f6c9e88e4f7ab264f4 **SHA-256 :** dd519b8f2efaf00cabe5cf0cfc0769f3e3a822feb9 **SHA-512 :** c34f13fd5420cee8738a042d5d1abf299d4fdf445 **Size :** 1.617 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** db0b0f67a8c376f0ffbdd5635d5ee5b5 **SHA-1 :** faca775c691ff7aa12321051d66a5e6d188a55a4 **SHA-256 :** 79bcf5d18573337235cd2ca6e7bcc88e0253797b **SHA-512 :** 4b10102519a2616f825804f61ceb83a3f89cfbc0a **Size :** 5.672 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Supdates.Db-Journal	**Type :** data **MD5 :** d6d9f08d99361060b01a08d24460bec1 **SHA-1 :** 457d46aa3fbb3c531cdafb82c72830b7e2071335 **SHA-256 :** c4875e46c4b2819041c13e76c20dab0bd051e4f1 **SHA-512 :** c3b5187bd780c39a1e09808ed4871cda0254719 **Size :** 1.544 Kilobytes.
C:\Users\User\AppData\Local\Temp\SlimCleanerPlus_en-US_x64_Silent.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 075a229499b5ceaa0f439d4a5f01ff08 **SHA-1 :** 91c5827500b047ef80fa23347d02bdc56e0bab22 **SHA-256 :** e9caeed965005ceee2c1e3284af4201b95c8f66d **SHA-512 :** a79c8e39cae531a8f4fb653239bedcdec282309ef **Size :** 18697.568 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Supdates.Db	**Type :** SQLite 3.x database **MD5 :** 502c79a63a307fe999ef82f77a1ceb97 **SHA-1 :** a94bde1e7e3a469e542041ed05c8a0a9ffdf7f52 **SHA-256 :** 638926cc308abe0d3187f03c815acec0c502e9fb1 **SHA-512 :** 7da85d9a97f11ef9130928bc2b34d95ac09990db **Size :** 8.192 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 0fe8c8dab5bd99c4b53f7bb321cd4557 **SHA-1 :** 4fd2fc16243cbce262ca1f08eb800efd24aaa508 **SHA-256 :** f64cb5e848beb6c76caca9b981c5cdfdba9b1281 **SHA-512 :** 5eec26308571db3cd19a0b6f2e5f916c1501e0d3 **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 5c0072b595a6cc78c741c084bf7cfc7b **SHA-1 :** 863a015d67ae2c9e8021e7cc821745edca2c0056 **SHA-256 :** 3e502a42d1f2a2c528b9ef0ca736133f524052e3 **SHA-512 :** d99ac27b89746cacfd9b089706d3dbc284dec728 **Size :** 1.544 Kilobytes.
C:\Users\User\AppData\Local\Temp\Swu2B56.Tmp	**Type :** bzip2 compressed data, block size = 900k **MD5 :** aaca9bff28318371a621f922da4c2af3 **SHA-1 :** 164c688c60c4c07810955bb30313d0ea16f5e07a **SHA-256 :** 34b002f8f0b461a3e6eaeb0fc821914e842939d7 **SHA-512 :** ebc0b076d81c4ece5b7f8cd7fdd0584b04dd1e79 **Size :** 3681.334 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** fdc558331b26c8b36428357f379412cd **SHA-1 :** 132df6fb7660d1edf3b3fe5cd7ac186e282745f3 **SHA-256 :** a5357db3317454a5630057ab9578472e216b5e9 **SHA-512 :** c349f65ef30d2272a017a5a85e3d27c79cb1adf7c **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** cdb185e98b47957efa1a9e60d8de69ba **SHA-1 :** e77119f2ae964a261bf3b94c08832ee188938231 **SHA-256 :** 52dfeb051dd6dce2e96176bff03b216669aa3f15 **SHA-512 :** 699aacbb22e2cb04a5cb02b455dce7b0d3ffd2f9 **Size :** 5.672 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Windows\Inf\Setupapi.App.Log	**Type :** ASCII text, with CRLF line terminators **MD5 :** c54f891f9e73f3d2f71a833c77ba44dc **SHA-1 :** d1bc91666dbb91c804f501cbe37dad9e30818b76 **SHA-256 :** 05392b98bc72f1cabc82b97c54110d029f3e9f51 **SHA-512 :** 20ab1479ac10101fed6dab3c4f17a8f588dd2344 **Size :** 106.206 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 204b88c11cfcab133f756f42b489293e **SHA-1 :** 7772269e33a69e691db2622403dd4945e9649eae **SHA-256 :** 7908a3e4d19d977ff400f52844b9a77a2c28fef69 **SHA-512 :** 2399579cae364241b1c56a669dfc3b1ea5969402 **Size :** 1.544 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 53cb6c26407437f5280b57812d6351c8 **SHA-1 :** be74113cd64010ba0c27fbf25b4102ef2061dcf8 **SHA-256 :** 71819a9756d015f01351b91857b7217eabe5fc51 **SHA-512 :** 0db175f7728fcf79f2fe3b3147022a3403cdfd52a **Size :** 2.576 Kilobytes.
C:\Windows\Tasks\DriverUpdate Scan.Job	**Type :** VAX-order 68k Blit mpx/mux executable **MD5 :** 1b5bdcfa84ddd8364444df2eeccc4168 **SHA-1 :** f237bc95c3285465daff944c2327ad342054c482 **SHA-256 :** 61e08064803dda017ad414da3b5b4bc08956f49 **SHA-512 :** ab1b01e0401fc5bab46726775cb528b73305f3b9 **Size :** 0.47 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** e4fb966e028ed2857a4d852d6e3758d5 **SHA-1 :** 75405a6a1b651b59fc2f3a18f73fc3d778db01d7 **SHA-256 :** 4f94b401fecc7b4f2a57f2a429bc44d1130612edb **SHA-512 :** 52dc7ac2639c96ad02871bd919dc566e9be99afc **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 0cd591598cca5e22be72c5ce1445b3fa **SHA-1 :** c032599c04f04be7371b20aece859edf4a58cdf5 **SHA-256 :** c76ca3f6e935654edd32bf821ee44a8e808a7dea **SHA-512 :** 0ed26ba66b0c7af7c20cc443744120095f0434a0 **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 1b2e4d74634447194c5e4f4474966b99 **SHA-1 :** d9856bc1a71998c5fdcc81c5e9cd258a28733e66 **SHA-256 :** adcede0010604b6e58c36ffe2386ca9d6d1804ed **SHA-512 :** 6a9ca9c7b907bedddf4b78000dcb91d5178e360 **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Supdates.Db-Journal	**Type :** dBase IV DBT, blocks size 3613630752, next free block index 4177909209 **MD5 :** 73d35946b491e384b08a220f88f22939 **SHA-1 :** ef0db0aca714705feeeafc1da12ceea87ce9f351 **SHA-256 :** 5e6eb8e5854fa1cae707de9ccc94345197e86521 **SHA-512 :** 5aa245ead50233a9a3b101e022fdc6bf6b8876b6 **Size :** 0.512 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** a5cf26154ea96d6c6bb5ec27462975de **SHA-1 :** 2b5eafb69621c71cca4e2502083bdc24a22cdff6 **SHA-256 :** 9996c11705d6f55b4d2d19641f02fe16ea9b875a **SHA-512 :** 7bd75f4a19379858edd0a23689cdf718420490d5 **Size :** 5.672 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** dBase IV DBT, blocks size 3613630752, next free block index 4177909209 **MD5 :** ad54afcb61b39973ebe574ab66583072 **SHA-1 :** d7b2628a1b59eba2c1cbb96f57e4337f525373eb **SHA-256 :** 9045f63ac6b5d6b869de5d523589532e37ec153 **SHA-512 :** 84c89e190c247559de7c94c49e1bdf5ac80d7671 **Size :** 0.512 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Supdates.Db-Journal	**Type :** data **MD5 :** 41a633225f22f08447bff5de1ff1e4aa **SHA-1 :** 3a2ebe268cb699f5de89fbe0487052f867567df4 **SHA-256 :** ab9c72825f6acd7728ae1a70d6abcebbf6edba7f **SHA-512 :** 7f950143c898c720163cab1c75e49da86da30462 **Size :** 1.544 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** bd73f4ebf38299d3c74f7d2d1d37e529 **SHA-1 :** d93750c156d7f0dd44d257555b239de5a82088bf **SHA-256 :** d3c597e43611998bdeca4723839e12778adda53 **SHA-512 :** b34ad6494dc7c68c53c21c1d292484c6023dd542 **Size :** 2.576 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 43dcac432f008ccad8380075aad80d3d **SHA-1 :** 39b0a391b2e9a17687a409ca9a736867507be56f **SHA-256 :** c2390ec47376625c127c2bbbd2acf21431a24761 **SHA-512 :** 599957bf4aebfa87520c76a1d2ac405758bc36c3 **Size :** 2.576 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 7ab98a745cf492610f006df3caa39f1f **SHA-1 :** 7379bb4988b9c98e4bbb4588d82c08388ed44c7b **SHA-256 :** f7e1de0a30d8badf54064462799547e7382bce66 **SHA-512 :** b8a5f3d7cf1295c70f52c385ae22d2c24ffc39bb26 **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 230db921503fa4f9273e1573ddd1fda4 **SHA-1 :** 2bf91558ddb1c5404d449619f32878b2adba72c1 **SHA-256 :** fc4030de4cbcd59fe806194e8feb7b858b3f51a23 **SHA-512 :** c737198f53b50b6c84dc47b210a7facc9b088b1b **Size :** 5.672 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 6aed3b8fc72b48733649501899129718 **SHA-1 :** 45d5f9504caf5a3ea3cf506e5aa019e0bfce0177 **SHA-256 :** 4eba5002bdf7d035b74216136693d51ff4b284d3 **SHA-512 :** 89e9ebfdfee3850f2396990e4113e468003fdec9e **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** d88e8f6a3ca97fbfd69cf73d8c21ee2b **SHA-1 :** 26e159568e225b0ade5a0b88e54a5af9e88c5592 **SHA-256 :** 95fac43f481c0c20b2f3f44e9a1b01e44ccd2176c2 **SHA-512 :** 0b7249475d2c3349d5e49e744f209dbeadaa13a **Size :** 5.672 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 1d5d8e3bd49061157e6fbd8edac196b5 **SHA-1 :** 03c7de65c2c17abd62ef1c977369145ba196f792 **SHA-256 :** 88a765d5c7de31c8482403e8ea86b28b7fe44f45 **SHA-512 :** 1897fc70968f8ef5264cde7e720d31b7f24a44347 **Size :** 2.576 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\9A19ADAD9D098E039450ABBEDD5616EB_90968CAB679DC8A66D51322A089E7CBE	**Type :** data **MD5 :** 180a5d561d7aa9a371376e1f0b2f02dc **SHA-1 :** d54134096ff852fbc66bd4f4bb2dd1c670633cb4 **SHA-256 :** c70a927ac799534c3dfd3332b4eb8da9e19b318e **SHA-512 :** 303d5a7bc2f596bd72545ac6ae246785a74d354a **Size :** 1.66 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** bed6064502194f5c8a67ec5da0e10e9a **SHA-1 :** e09cf7b85b70f0677bae70a1a002f1c87c0bdc46 **SHA-256 :** 65f768002d3e96efe6fe6ec1534d12f2120029a18 **SHA-512 :** 997cc42c88fd5cb5e9a3202f2b917a9743948379(**Size :** 5.672 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Logs\2018-08-07 19-20-29 0.Log	**Type :** ASCII text, with CRLF line terminators **MD5 :** a902a21320cddbec18951639db198d4e **SHA-1 :** 3cf09dca846491de1ddfa6e08bf5e7457e87f7ad **SHA-256 :** 0a2bbbbf4fa4968d56384c6be05949354d909293 **SHA-512 :** c4fbdaf7aa588e8cdcc5ba1e87fa316c8c9e76763 **Size :** 0.124 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Supdates.Db-Journal	**Type :** data **MD5 :** 5fd8414510bcefea1fb95c327a968b21 **SHA-1 :** 6e820365eb151df994d472fddf980ffa910df7e0 **SHA-256 :** 33e80c283581929198871a0bee4710669bb9a6d **SHA-512 :** 71c8f9e6992986143777f2144b5c6ba141f68d7a(**Size :** 1.544 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** c61ba50951d5cca90a1c6635d56c9574 **SHA-1 :** 9637c031e552e52611cc5c8c708cf84aed12d7e7 **SHA-256 :** f72d978d63c390602bd73fa3bf733896df2223fa5 **SHA-512 :** 7ced3e0b19dd6666b2f30618ecdb7ad863318446 **Size :** 2.576 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 271ad0006b1669e48b204837d3a4c8a2 **SHA-1 :** d2a1fa871c709b1166db92d1941097efe1a5f9bf **SHA-256 :** 28bf9d9a5fbc08b8522caba893865c6ca3511c1d3 **SHA-512 :** 1ff150b99290edc06c859cf289d4491f5aa040279 **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\SWDUMon.Inf	**Type :** ASCII text, with CRLF line terminators **MD5 :** b65ddb94d2d123934de74e627ccc663c **SHA-1 :** e4a6427eed2e35df1f77476e65af1caa4b8a1a37 **SHA-256 :** 26f246efad9dbde96fa3ca39352e986deb31bf35(**SHA-512 :** 408139262086c4c9e8b5b255017c101ecc6199f8 **Size :** 1.639 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db	**Type :** SQLite 3.x database **MD5 :** 2c0c6be24b63bf2d1df014fbea398a47 **SHA-1 :** 481c9ea7f0891a533de40ee9da503c1a4e1065cd **SHA-256 :** 4da99635e94ec0e79f3f33ebd3f6d904d8c99c608 **SHA-512 :** 61bc3ecc7e46b07a9ef01025e21148c4fa0950bc4 **Size :** 9.216 Kilobytes.
C:\Users\User\AppData\Local\Temp\MSI4909.LOG	**Type :** Little-endian UTF-16 Unicode text, with very long lines, with CRLF line terminators **MD5 :** e890efe221bf46e2fd0a3b52f45ed71d **SHA-1 :** 489d4aa89edef82b5156e99d07b138c350bbd5b3 **SHA-256 :** 12bbc9e8a52a7dfc66bf5cda1bc2e2af870e5d09(**SHA-512 :** 8d8e26ccbe192b440f15f584275d022c849df8a3a **Size :** 144.8 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 1c99c4b01ab1f5a3afa3a8450f51f81e **SHA-1 :** a1e2103c959fc7fa679da91fede833de3b6b3218 **SHA-256 :** a204fbd2d701e77916b77286981b92dbf95eae5 **SHA-512 :** 73861579f44f220c8372d8b715bb08f93983870c **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\SWDUMon.Cat	**Type :** data **MD5 :** 0b1da72305373dba342a749ce9a4402e **SHA-1 :** 8db059f27c70193cf9f71cd3f72f5f2db2528ddf **SHA-256 :** 60a36a7d6ad77d392b355950fb6877f804be0a1 **SHA-512 :** ad64ea8e4a01b25b3c0124f7f462f137198550cfa **Size :** 7.584 Kilobytes.
C:\Users\User\AppData\Local\Temp\MSI1281e.LOG	**Type :** Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators **MD5 :** 0140e0504409b378bedd8c6afdf99ba8 **SHA-1 :** 5edf33216f3d8b6d818edd2f55f66feef6691d69 **SHA-256 :** 9abbe1ab2ce21c1052bd1b285c641011f1794e9e **SHA-512 :** ee5fd6efbb046384937f51f46817b7ba22635677 **Size :** 305.578 Kilobytes.
C:\Windows\Sysnative\Tasks\DriverUpdate Startup	**Type :** XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators **MD5 :** 3cbe2aab36a7bccedcab755b2c7c4901 **SHA-1 :** 0e2f73aefa1a13ea59918910543e4b93d614464a **SHA-256 :** 840e7326d33ac2b41c632b7002e31c77fa68f298 **SHA-512 :** 99a8109620905f7e94124a22f80f01db292c578e **Size :** 2.84 Kilobytes.
C:\Users\User\AppData\Local\Temp\SIOUT35716500\SlimCleanerPlus_en-US_x64.Msi **C:\Users\User\AppData\Local\Downloaded Installers\{7E03DFCF-3091-4D7A-91AB-59994A7A36B6}\Setup.Msi**	**Type :** Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Title: Installation Database, Subject: SlimCleaner Plus, Author: Slimware Utilities Holdings, Inc., Keywords: Installer, Comments: This installer database contains the logic and data required to install SlimCleaner Plus., Template: x64;1033, Revision Number: {B95C2D48-FDF6-4969-B6C3-EC3D8C7F854F}, Create Time/Date: Mon Jun 18 13:15:38 2018, Last Saved Time/Date: Mon Jun 18 13:15:38 2018, Number of Pages: 200, Number of Words: 2, Name of Creating Application: Windows Installer XML Toolset (3.11.0.1701), Security: 2 **MD5 :** e06f060862460b552006a57bcfcfe21b **SHA-1 :** b4f7224c4363461cc9c13e0064a0ad212a4c17ea **SHA-256 :** b189cd46996293761cd8ef343d308a72d1e08dc6 **SHA-512 :** e2557944188aad54562bac56b8d13b0cbd9613d **Size :** 48455.68 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** a5521367c1160f996c3ad33be8c889ca **SHA-1 :** 450704cd98cbb742acf23f9a3aec6358120244ed **SHA-256 :** c5442e5b1fad6f48af773463a2a6161020842430 **SHA-512 :** 0dc3d91927e7ed0e0e07a7777bf5fe67fe22b947 **Size :** 6.704 Kilobytes.
C:\Windows\Tasks\DriverUpdate Startup.Job	**Type :** VAX-order 68k Blit mpx/mux executable **MD5 :** cac0841f3613c969361ac51e9ab6cf1a **SHA-1 :** b609fb46eb78f84700c6270ffd7e058d5cefa941 **SHA-256 :** c32066b6a409629d3b3d5c0c4b42409a5b72317 **SHA-512 :** 341125559b1ccae1d22b6a48f9a5b029fac064bc **Size :** 0.416 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 0bdce5a1903d24267b8c5223654576ab **SHA-1 :** a78b626089cf17c04ece6ac2b12f4968bcc6ed53 **SHA-256 :** 657f2c106eca54bb13f438cf8dfc4d07fca5998e1f **SHA-512 :** 53a3100743d966d0f6e996d821a477b79b4339f9 **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\Temp\Scp3C30.Tmp	**Type :** bzip2 compressed data, block size = 900k **MD5 :** d24a8f32dbd71500fe2d23e7bcfa9036 **SHA-1 :** 9cc6af92eac3b6d1691c397055487b45f79c3ccd **SHA-256 :** 3f8da3a70c339548d603962a41bf24f3c6ff576fec **SHA-512 :** 0a7d6df2170597c3096dc1332f4afb55e5ad40d7 **Size :** 138.304 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\SWDUMon.Sys **C:\Windows\Sysnative\Drivers\SWDUMon.Sys**	**Type :** PE32+ executable (native) x86-64, for MS Windows **MD5 :** 04cf20310145dec63d5387beaff77d9a **SHA-1 :** 1e0e9f8751402b3484f765e0709209e2a96e9f5c **SHA-256 :** 5017af8c2dfbfe1f9946ff5af229d62d141118ea92 **SHA-512 :** e3c3b4409d31fdbdf9184c58e01845dc8e4664c0 **Size :** 13.92 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Images\Acer.Png	**Type :** PNG image data, 50 x 50, 8-bit/color RGBA, non-interlaced **MD5 :** 7f82dcde9e8771dc032c21a693a8ecd1 **SHA-1 :** 8aa59c0277bc615d5eb63cd52af6e400fae02940 **SHA-256 :** d3d820ac11b1f30d4ccef16556e35c42f7b71c97c **SHA-512 :** 70fa188153de052122b7dc5a00d2973686b5708 **Size :** 2.011 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** bb7d1bd7d4d9c4dd2ee2536a2d7274ac **SHA-1 :** 6a906e0d248b70f6ce4fa5bf6257d50f35e9b250 **SHA-256 :** f870567c2b6283ab28f9ccf6e6bfa02977dc0ab3f5 **SHA-512 :** aa18302a52d840f15f919694faa0f45a1b5a18c5b **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\9A19ADAD9D098E039450ABBEDD5616EB_90968CAB679DC8A66D51322A089E7CBE	**Type :** data **MD5 :** 1b517a03b3f9c453cf7e29fd106636cf **SHA-1 :** 838a39514fb668fd74975d7edea10967fc5c1de4 **SHA-256 :** b438523a043bdfe2a253b66688910b3862ace70 **SHA-512 :** fee38d42c332d65bcb89eb4d00e65c00c302f29a **Size :** 0.398 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 2f0ad9d0a44335bd665063a8e7f3eb2b **SHA-1 :** 00dd34cd19dd9ded8ab9380baff34babb49edde9 **SHA-256 :** f624d0f80019d6952f16640a9e9c7e7c30ae7aba1 **SHA-512 :** 72cb217d038bce7b2efc81c07b770320e924d099 **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 8fff177b031c4a2511260e95126b2737 **SHA-1 :** 9d49b47a8d48c79d5f0cc09295dbfb212232976a **SHA-256 :** 4dfe9108f4f1ddf482fecf272b539f5557a4bbb941 **SHA-512 :** 914f4dc76c8e31e440108332cdc4829c9c9bdec98 **Size :** 2.576 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Swu2B56.Tmp.Msi **C:\Users\Public\Documents\Downloaded Installers\{055C7DA5-A1F5-41FB-932C-82474ED3487A}\Setup.Msi**	**Type :** Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.3, Code page: 1252, Title: Installation Database, Subject: Looks for updates for your computer's software and drivers to improve performance., Author: Slimware Utilities Holdings, Inc., Keywords: update, software, drivers, Comments: This installer database contains the logic and data required to install DriverUpdate., Template: Intel;1033, Revision Number: {8BA6BC7B-FA09-46C3-8633-322698E0999B}, Create Time/Date: Wed Jul 19 18:02:22 2017, Last Saved Time/Date: Wed Jul 19 18:02:22 2017, Number of Pages: 200, Number of Words: 2, Name of Creating Application: Windows Installer XML Toolset (3.9.1208.0), Security: 2 **MD5 :** 2dfb22e30d15b09ffd03997ca388ad19 **SHA-1 :** fb66ebb7cbdb3644585c3261800f951c492475f2 **SHA-256 :** e532c509b45f15c469c0186dd26b68f1e0502476 **SHA-512 :** 0444bd12ab254931ff86ed948b3e0cfa8da88c1fe **Size :** 30523.392 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 255ad1fbed91e1f17100ebc488984c2f **SHA-1 :** 133f0707975c1ab3f8b2dab6b3707e61a77bedc5 **SHA-256 :** babbea282c7921aff38ae769592cd1be36884d26 **SHA-512 :** b2cb4c8e610f777eab26857d8520a0aa624dad82 **Size :** 6.704 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	RIFZBJX.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	917b2f646ee7700f1e38d42a8810f67c9633c83a
MD5:	ec46453ecc39a9798562226d5c580ff5
First Seen Date:	2016-10-19 05:55:41.956384 (2 years ago)
Number Of Clients Seen:	2
Last Analysis Date:	2018-08-04 15:59:48.828804 (7 months 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	[{u'Path': u'E:\\BuildAgent\\work\\cdc3d0ebfd4f8694\\bin\\Release\\LittleInstaller.pdb\x00', u'GUID': u'{d63146b1-b27d-40b7-ba24-b38b444939be}', u'timestamp': u'2015-10-27 14:07:51'}]
Number Of Sections	5
Trid	[[54.3, u'InstallShield setup'], [34.8, u'Win64 Executable (generic)'], [5.6, u'Win32 Executable (generic)'], [2.5, u'Generic Win/DOS Executable'], [2.5, u'DOS Executable Generic']]
Compilation Time Stamp	0x562F8537 [Tue Oct 27 14:07:51 2015 UTC]
LegalCopyright	Copyright Slimware Utilities, Inc. 2011-2015
InternalName	LittleInstaller
FileVersion	2.5.0
CompanyName	Slimware Utilities, Inc.
ProductName	DriverUpdate
ProductVersion	2.5.0
FileDescription	DriverUpdate Setup Wizard
OriginalFilename	DriverUpdate-setup.exe
Translation	0x0409 0x04b0
Entry Point	0x43508f (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	961376
Ssdeep	12288:BHwvQ2XK9Vh8j/hKX/tXKTYvnqFo78CcCUKmu7b:a4gdK1kYvb8C5R77b
Sha256	a8ca3daca4a8caee5e7e0b29a26a3fecd0200912b605bf70a4f2ceeafaba2a60
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/9/1/7/b/917b2f646ee7700f1e38d42a8810f67c9633c83a', u'EXE:OriginalFileName': u'DriverUpdate-setup.exe', u'EXE:ProductName': u'DriverUpdate', u'EXE:InternalName': u'LittleInstaller', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:08:04 14:15:04+00:00', u'EXE:InitializedDataSize': 634880, u'File:FileModifyDate': u'2018:08:04 14:15:04+00:00', u'EXE:FileVersionNumber': u'2.5.0.0', u'EXE:FileVersion': u'2.5.0', u'File:FileSize': u'939 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Windows NT 32-bit', u'EXE:ProductVersion': u'2.5.0', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'Slimware Utilities, Inc.', u'File:FileName': u'917b2f646ee7700f1e38d42a8810f67c9633c83a', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2015:10:27 14:07:51+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Copyright Slimware Utilities, Inc. 2011-2015', u'EXE:LinkerVersion': 8.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/9/1/7/b', u'EXE:FileDescription': u'DriverUpdate Setup Wizard', u'EXE:EntryPoint': u'0x3508f', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 331776, u'File:FileInodeChangeDate': u'2018:08:04 14:15:04+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'2.5.0.0'}]
Mime Type	application/x-dosexec
Imphash	0553028fe8bd07ea4e1f68bf6556dfcd

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x50cea	0x51000	6.62881943135	8abcad4ba7fed585e40398d6ea7d01b7
.rdata	0x52000	0x167c2	0x17000	4.64798331138	476669dee0523e50d64534bcafacb92f
.data	0x69000	0x7c5c	0x4000	4.54716977183	d897bfcfd1c32e42a855466389abba40
.rsrc	0x71000	0x6e092	0x6f000	5.81179496162	fab55575f24b8a510700830c58c6e656
.reloc	0xe0000	0xc3fe	0xd000	3.90964485022	43836d43f47ec512bf5928e18aed4aef

PE Imports

- KERNEL32.dll
  - TlsFree
  - SetErrorMode
  - HeapFree
  - HeapAlloc
  - GetProcessHeap
  - GetStartupInfoW
  - ExitProcess
  - HeapReAlloc
  - RtlUnwind
  - SetStdHandle
  - GetFileType
  - ExitThread
  - CreateThread
  - HeapSize
  - VirtualAlloc
  - SetUnhandledExceptionFilter
  - GetStdHandle
  - GetModuleFileNameA
  - FreeEnvironmentStringsA
  - GetEnvironmentStrings
  - FreeEnvironmentStringsW
  - GetEnvironmentStringsW
  - GetCommandLineA
  - GetCommandLineW
  - LocalReAlloc
  - GetStartupInfoA
  - HeapDestroy
  - HeapCreate
  - VirtualFree
  - QueryPerformanceCounter
  - GetSystemTimeAsFileTime
  - TerminateProcess
  - UnhandledExceptionFilter
  - IsDebuggerPresent
  - GetCPInfo
  - GetACP
  - GetOEMCP
  - IsValidCodePage
  - GetTimeFormatA
  - GetDateFormatA
  - GetTimeZoneInformation
  - LCMapStringA
  - LCMapStringW
  - GetConsoleCP
  - GetConsoleMode
  - GetStringTypeA
  - GetStringTypeW
  - GetLocaleInfoA
  - WriteConsoleA
  - GetConsoleOutputCP
  - WriteConsoleW
  - CreateFileA
  - SetEnvironmentVariableA
  - TlsSetValue
  - TlsAlloc
  - GlobalHandle
  - GlobalReAlloc
  - TlsGetValue

- GlobalFlags
- WritePrivateProfileStringW
- ReleaseMutex
- CreateMutexW
- GetCurrentThread
- ConvertDefaultLocale
- GetVersion
- EnumResourceLanguagesW
- GetLocaleInfoW
- LoadLibraryExW
- CompareStringA
- InterlockedExchange
- CreateEventW
- SuspendThread
- SetEvent
- ResumeThread
- SetThreadPriority
- lstrcmpA
- GetFullPathNameW
- GetVolumeInformationW
- DuplicateHandle
- SetEndOfFile
- UnlockFile
- LockFile
- WriteFile
- GetThreadLocale
- GetFileTime
- GetFileAttributesW
- FindFirstFileW
- FindClose
- GetModuleHandleA
- GlobalAddAtomW
- GlobalFindAtomW
- GlobalDeleteAtom
- FreeLibrary
- CompareStringW
- LoadLibraryA
- lstrcmpW
- GetVersionExA
- GlobalLock
- GlobalUnlock
- FreeResource
- GlobalAlloc
- GlobalFree
- lstrlenA
- LocalAlloc
- FindResourceExW
- GetFileSize
- CreateFileMappingW
- MapViewOfFileEx
- UnmapViewOfFile
- GetFileSizeEx
- WideCharToMultiByte
- ExpandEnvironmentStringsW
- InterlockedDecrement
- InterlockedIncrement
- DeleteCriticalSection
- LeaveCriticalSection
- InitializeCriticalSection
- MoveFileExW
- EnterCriticalSection
- GetCurrentProcessId
- GetCurrentThreadId
- CreateFileW
- DeleteFileW
- RaiseException
- ReadFile
- SetFilePointer
- FlushFileBuffers
- GetCurrentProcess
- VerSetConditionMask
- VerifyVersionInfoW
- CopyFileW
- CreateDirectoryW
- MultiByteToWideChar

    - GetTickCount
    - GetTempFileNameW
    - GetTempPathW
    - CloseHandle
    - OpenEventW
    - CreateProcessW
    - lstrlenW
    - GetUserDefaultUILanguage
    - MulDiv
    - GetVersionExW
    - WaitForSingleObject
    - Sleep
    - FileTimeToLocalFileTime
    - FileTimeToSystemTime
    - GetUserDefaultLangID
    - GetModuleFileNameW
    - GetProcAddress
    - LoadLibraryW
    - SetLastError
    - LocalHandle
    - GetModuleHandleW
    - GetLastError
    - FormatMessageW
    - FindResourceW
    - LoadResource
    - LockResource
    - SizeofResource
    - SetHandleCount
    - LocalFree
- USER32.dll
    - DestroyMenu
    - GetMessageW
    - TranslateMessage
    - ValidateRect
    - CharUpperW
    - EndPaint
    - BeginPaint
    - RegisterWindowMessageW
    - SendDlgItemMessageA
    - WinHelpW
    - GetCapture
    - SetWindowsHookExW
    - CallNextHookEx
    - GetClassLongW
    - SetPropW
    - GetPropW
    - RemovePropW
    - GetLastActivePopup
    - DispatchMessageW
    - GetTopWindow
    - UnhookWindowsHookEx
    - GetMessageTime
    - GetMessagePos
    - PeekMessageW
    - MapWindowPoints
    - GetKeyState
    - SetForegroundWindow
    - UpdateWindow
    - GetMenu
    - GetSubMenu
    - GetMenuItemID
    - GetMenuItemCount
    - CreateWindowExW
    - GetClassInfoExW
    - GetClassInfoW
    - RegisterClassW
    - DefWindowProcW
    - CallWindowProcW
    - SystemParametersInfoA
    - IsIconic
    - GetWindowPlacement
    - GetWindowTextW
    - SetWindowPos
    - SetFocus
    - MoveWindow

- IsDialogMessageW
- IsDlgButtonChecked
- SetDlgItemTextW
- SendDlgItemMessageW
- CheckDlgButton
- GetDesktopWindow
- GetActiveWindow
- SetActiveWindow
- GetSystemMetrics
- CreateDialogIndirectParamW
- DestroyWindow
- GetDlgItem
- IsWindowEnabled
- GetNextDlgTabItem
- EndDialog
- SetMenuItemBitmaps
- GetMenuCheckMarkDimensions
- LoadBitmapW
- GetFocus
- ModifyMenuW
- RegisterClipboardFormatW
- GetMenuState
- CheckMenuItem
- EnumThreadWindows
- WaitForInputIdle
- ShowWindow
- KillTimer
- SetTimer
- InvalidateRect
- ReleaseDC
- GetDC
- ClientToScreen
- ScreenToClient
- ReleaseCapture
- SetCapture
- PtInRect
- TrackMouseEvent
- LoadCursorW
- SetCursor
- SetRectEmpty
- GetClassNameW
- GetDlgCtrlID
- GetSysColorBrush
- SetWindowTextW
- UnregisterClassW
- EnumChildWindows
- FillRect
- GetClientRect
- IsWindowVisible
- MessageBoxW
- GetWindowThreadProcessId
- DestroyAcceleratorTable
- GetParent
- TranslateAcceleratorW
- OffsetRect
- EnableMenuItem
- AdjustWindowRectEx
- CreateAcceleratorTableW
- SetRect
- MessageBeep
- MapDialogRect
- GetCursorPos
- IsWindow
- GrayStringW
- DrawTextExW
- DrawTextW
- TabbedTextOutW
- GetForegroundWindow
- PostMessageW
- AppendMenuW
- GetSystemMenu
- LoadIconW
- GetWindowLongW
- SetWindowLongW
- PostQuitMessage

    - PostThreadMessageW
    - GetWindow
    - CloseWindow
    - GetSysColor
    - IsRectEmpty
    - CopyRect
    - RedrawWindow
    - GetWindowRect
    - SendMessageW
    - EnableWindow
    - GetWindowTextLengthW
    - UnregisterClassA
- GDI32.dll
    - GetStockObject
    - DPtoLP
    - DeleteDC
    - MoveToEx
    - LineTo
    - ScaleWindowExtEx
    - SetWindowExtEx
    - ScaleViewportExtEx
    - SetViewportExtEx
    - OffsetViewportOrgEx
    - SetViewportOrgEx
    - SelectObject
    - CreateDIBSection
    - SetMapMode
    - SetBkMode
    - RestoreDC
    - SaveDC
    - SetBkColor
    - SetTextColor
    - GetClipBox
    - CreateBitmap
    - SelectClipRgn
    - GetTextExtentExPointW
    - CreateCompatibleBitmap
    - BitBlt
    - SetBrushOrgEx
    - CreateCompatibleDC
    - CreatePatternBrush
    - GetDeviceCaps
    - CreatePen
    - CreateSolidBrush
    - GetTextMetricsW
    - Rectangle
    - ExtTextOutW
    - TextOutW
    - RectVisible
    - PtVisible
    - Escape
    - GetObjectW
    - CreateFontIndirectW
    - GetTextExtentPoint32W
    - DeleteObject
- COMDLG32.dll
    - GetFileTitleW
- WINSPOOL.DRV
    - OpenPrinterW
    - ClosePrinter
    - DocumentPropertiesW
- ADVAPI32.dll
    - RegEnumKeyExW
    - RegQueryValueW
    - RegEnumKeyW
    - RegDeleteKeyW
    - RegOpenKeyW
    - RegDeleteValueW
    - RegEnumValueW
    - RegCloseKey
    - RegQueryInfoKeyW
    - RegSetValueExW
    - RegCreateKeyExW
    - RegQueryValueExW
    - RegOpenKeyExW

- SHELL32.dll
  - ShellExecuteW
  - SHGetFolderPathW
  - CommandLineToArgvW
  - Shell_NotifyIconW
- COMCTL32.dll
  - InitCommonControlsEx
- SHLWAPI.dll
  - PathAppendW
  - UrlEscapeA
  - SHCreateStreamOnFileEx
  - AssocQueryStringW
  - PathStripToRootW
  - PathIsUNCW
  - PathFindFileNameW
  - PathFindExtensionW
  - PathFileExistsW
- oledlg.dll
  - OleUIBusyW
- ole32.dll
  - CoRegisterMessageFilter
  - OleFlushClipboard
  - OleIsCurrentClipboard
  - CoRevokeClassObject
  - OleInitialize
  - CoFreeUnusedLibraries
  - OleUninitialize
  - CoInitialize
  - CoUninitialize
  - StringFromGUID2
  - CoInitializeEx
  - CoCreateGuid
  - CreateStreamOnHGlobal
  - CoCreateInstance
- OLEAUT32.dll
  - VariantChangeType
  - SysStringLen
  - SysAllocStringLen
  - LoadTypeLib
  - SysFreeString
  - VariantInit
  - SysAllocString
  - VariantClear
  - LoadRegTypeLib
- WINHTTP.dll
  - WinHttpReadData
  - WinHttpGetProxyForUrl
  - WinHttpDetectAutoProxyConfigUrl
  - WinHttpGetIEProxyConfigForCurrentUser
  - WinHttpConnect
  - WinHttpOpen
  - WinHttpReceiveResponse
  - WinHttpSendRequest
  - WinHttpQueryHeaders
  - WinHttpSetOption
  - WinHttpCloseHandle
  - WinHttpOpenRequest
- VERSION.dll
  - VerQueryValueW
  - GetFileVersionInfoW
  - GetFileVersionInfoSizeW
- msi.dll
  - None
  - None
  - None
  - None
  - None
  - None
  - None
  - None
  - None
  - None
- RICHED20.dll
  - None
- gdiplus.dll

- GdipCloneImage
- GdipDrawImageRectI
- GdipCreateFromHDC
- GdipCreateBitmapFromHBITMAP
- GdipAlloc
- GdipDisposeImage
- GdiplusShutdown
- GdiplusStartup
- GdipFree
- GdipDeleteGraphics

- WS2_32.dll
  - WSAStartup
- OLEACC.dll
  - LresultFromObject
  - CreateStdAccessibleObject

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 467712, u'sha256': u'fbeb3be87e80cb8e1d2af3d8140796c1bb80c6c7056f60897088ff9e355c3867', u'type': u'data', u'size': 308}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 468020, u'sha256': u'f64ccc0582bc7c66af8b40049e485e8e241335261ec95ace909293ba50b2e4a3', u'type': u'data', u'size': 180}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 468200, u'sha256': u'e7c0005285d1ab59732d5f99f77a9bdd6342b01cf44437ebd7a07611a227e272', u'type': u'data', u'size': 184}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 468384, u'sha256': u'abdf36bde89a26349f5741c17c235dacea88d441d8662ba16a598dc50c3c4864', u'type': u'data', u'size': 324}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 468708, u'sha256': u'ca8fc96218d0a7e691dd7b95da05a27246439822d09b829af240523b28fd5bb3', u'type': u'data', u'size': 744}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 469452, u'sha256': u'f59f62e7843b3ff992cf769a3c608acd4a85a38b3b302cda8507b75163659d7b', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 469748, u'sha256': u'3bbacbad1458254c59ad7d0fd9bea998d46b70b8f8dcfc56aad561a293ffdae3', u'type': u'data', u'size': 2216}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 471964, u'sha256': u'dc785b2a3e4ea82bd34121cc04e80758e221f11ee686fcfd87ce49f8e6730b22', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 473348, u'sha256': u'6e4c3f9044eaf9d157ec8e50bc8a5cd9069b6078058094a4b4a4ab8e6e1ffac1', u'type': u'data', u'size': 68}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 473416, u'sha256': u'300f275bbb1008b2a4367954d64a08db87c680c7bdd0c03615c3a37cfc61a0a9', u'type': u'data', u'size': 366}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 473784, u'sha256': u'4f74a949fe2c9358a546f41a9c598fbe326b432ff17dfbacf2842ac6e7d1787a', u'type': u'data', u'size': 332}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 474116, u'sha256': u'b89eec935455ed0f590248a8446072a56ccc12ab66583b2e54719ec5cf4e2bc1', u'type': u'data', u'size': 362}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 474480, u'sha256': u'62baabd903384fbf221e1149d05900356bd2286c2567e2ce231ee7d168692afe', u'type': u'data', u'size': 526}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 475008, u'sha256': u'e33eb3d08a57cf5dd3710ff2252141f2723984ab13fbebddd2db86f2747ba929', u'type': u'data', u'size': 320}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 475328, u'sha256': u'3b442c077a3c0edd83101d47295701259db768024978619fce3b978e4ccdebdc', u'type': u'data', u'size': 462}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 475792, u'sha256': u'd740b552c6f5879f3193780de45a419aea68ed0e24f1ae2857115f661adc3052', u'type': u'data', u'size': 376}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 476168, u'sha256': u'e16f477b8e47cb4ad9028fb34bb451bdb85c6a8b5bd7f8b18a8088564983e43c', u'type': u'data', u'size': 534}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 476704, u'sha256': u'0da23009e825ebab541af8804f12bf6d64497bd2efb4635a6b8b97ebbb9c84b0', u'type': u'data', u'size': 518}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 477224, u'sha256': u'4cf716efaf68e0cb2ec45ec55d291050b5712b05653cae68edbb999f803d2a98', u'type': u'data', u'size': 52}

{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 477276, u'sha256': u'ef0bd5e1ffda4669aaecfe0012902695f6c2b037faef45041e01f46432ec75fd', u'type': u'MS Windows cursor resource - 79 icons, 75x256, hotspot @65x98', u'size': 218}

{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 477496, u'sha256': u'624ca146b3e88682a3e3bcfc7dcdfdb6193334bc25dd012c68cf715848f2df7d', u'type': u'MS Windows cursor resource - 79 icons, 75x256, hotspot @67x97', u'size': 212}

{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 477708, u'sha256': u'4fd87b49fb1dd0e7f6732264c0bc292ce6aae422c692af72315fd455739d5f5a', u'type': u'MS Windows cursor resource - 79 icons, 75x256, hotspot @65x110', u'size': 204}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 477912, u'sha256': u'040be5bce4d9275ba3d7123d4d87665b1aa9c4acd4a5885d5dc56dd29dd9cebf', u'type': u'MS Windows cursor resource - 79 icons, 75x256, hotspot @67x97', u'size': 172}

{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 478084, u'sha256': u'61b693adfd5c4b4077c78c1e56f1723e9dc91c78aaf50cdb900bb617de4c6623', u'type': u'MS Windows cursor resource - 79 icons, 75x256, hotspot @12461x12515', u'size': 96}

{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 478180, u'sha256': u'4803a1975883eb60af94b51e9532e228976461273c7371f3cd133aa4e785819b', u'type': u'data', u'size': 98}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 478280, u'sha256': u'f39b611bd7fd6cf6911947fec504ddde1603149502b794c3f8bb28aa4c088c5f', u'type': u'data', u'size': 120}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 478400, u'sha256': u'ba847dbbcbb4d05fcf8c5c6ca8dbe2e8f1bef3c8ba5bd1862fe1644b2dd73156', u'type': u'data', u'size': 128}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 478528, u'sha256': u'81f3a5cb443e8ad28345f14d4f2ff55aae85e56f3058489e75172ca1164e131d', u'type': u'data', u'size': 82}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 478612, u'sha256': u'258d51f0e31fb7e76662e90b0b6f7276eea18dd7be38bb2f37a883617db56c7a', u'type': u'data', u'size': 68}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 478680, u'sha256': u'08c792e3e0c8c773892a51fc5f1acfabd6bf5556e5e05f33c728e8bec4577610', u'type': u'data', u'size': 258}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 478940, u'sha256': u'da54b5e20f2459b9a25d8b22005d66a8a24dcfdbf5fca99893d5d08515d25586', u'type': u'data', u'size': 314}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 479256, u'sha256': u'fc0ac66e26e5951aa62080e9f15920e54c6aded25923c43f401b69f232a940a6', u'type': u'data', u'size': 340}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 479596, u'sha256': u'897f48ffd80577b462e07038911df69b1607a270b0d83a024c0b7a78361d6aee', u'type': u'data', u'size': 228}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 479824, u'sha256': u'f5f2d753d1a3986f3ce3a955d2b2a1d5af05c5dc69e3a6567f8b75541f0f0db0', u'type': u'data', u'size': 174}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 480000, u'sha256': u'40c1b95e6f501edd0ebff2a2736f38e94f9930b76bfe0a28fed3dd62b1ab47c8', u'type': u'data', u'size': 594}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 480596, u'sha256': u'1056298d4517e7cedfe80bac785d9a4e0fc7b4df0bd1847bf1727a3c259aa2b8', u'type': u'data', u'size': 480}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 481076, u'sha256': u'06025e6f9616ddd627cdca09aac5653e9c890e03c8408f8d4db58a8883c9f19a', u'type': u'data', u'size': 516}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 481592, u'sha256': u'1e5598008e22ef78ff73e17947e5980ffbfbbe8f7d5dd3cf2d8e34e28f175eeb', u'type': u'data', u'size': 380}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 481972, u'sha256': u'309f434d357a58c314d921e23f3411e90628698a9375dfe689281617ff688267', u'type': u'data', u'size': 228}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 482200, u'sha256': u'fe3776e5253ea7c3f7f1803cf553591008606baf3d1a67783185a3ad5d89d7c7', u'type': u'data', u'size': 894}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 483096, u'sha256': u'8426b361567dd1b05cb4d942609fbb83c33a8aee657f70898d89ae24b87c226c', u'type': u'data', u'size': 884}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 483980, u'sha256': u'931d781835f6843bc9d41ab728b2209fca69b28af9b805b625375fc06d11368e', u'type': u'data', u'size': 910}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 484892, u'sha256': u'172d61402c2619a2142e152c771acb8f555386043cea2a66dc747b2cc171446e', u'type': u'data', u'size': 690}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 485584, u'sha256': u'72a5e421c5be5e4afa90b7caf3294a45a98ab6821d265a65adbcf63344036019', u'type': u'data', u'size': 526}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 486112, u'sha256': u'84050bef84e46fe781f9c5ac7cb30985aef90b23beb97bc425a6fae49cf3cb6a', u'type': u'data', u'size': 290}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 486404, u'sha256': u'ad279e11c370d3e636cf8167bef1a9ea82282bccd80431a100c86d314297d25c', u'type': u'data', u'size': 284}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 486688, u'sha256': u'8d88449cff57219d23f311779473047b16e7efe62f8077e5f053b40931358c0b', u'type': u'data', u'size': 286}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 486976, u'sha256': u'90473bb9384f3f39541eabad15e612fe7c8cd555cbca23fbb06d05ac90aa29a3', u'type': u'data', u'size': 296}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 487272, u'sha256': u'814bebef4ed9fd87c501e2d52feef223193d9a9859a9d0e9a9beca3b69ef7012', u'type': u'data', u'size': 212}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 487484, u'sha256': u'0947cde4cd80ac726e4d7d5d5d966bf16ea1dba641df74265d529724d369d33f', u'type': u'data', u'size': 378}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 487864, u'sha256': u'b69faeb1cc99f8532806c8bf35d553b6ca8293fe32bbd7bd1e2cdfa3d19096ed', u'type': u'data', u'size': 360}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 488224, u'sha256': u'a246ce2c4837b1fbe3d54ed158ffd8fe727105418327bd1f8029263365005412', u'type': u'data', u'size': 344}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 488568, u'sha256': u'fb8e67ea0b8787e4ed24ca15731be79548d684699746bc53a8d3e228f4e71de1', u'type': u'data', u'size': 280}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 488848, u'sha256': u'a7e3c29df3af8134eb884624ec3636b227f5b922d703c3129221986366a749e1', u'type': u'data', u'size': 172}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 489020, u'sha256': u'2ad80490bfbd67e316b34a78c166dfbc8ddbbbac2ac5d3232692fc77dfa32de1', u'type': u'data', u'size': 438}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 489460, u'sha256': u'2cfe0e6e9d5cd1695f2f1028e9936286288f0408d246457ce99509303c1f908f', u'type': u'data', u'size': 426}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 489888, u'sha256': u'fcadde9f221c77e92a26007a43313154e345e09d952ebf6adfa84d2341cc8fa7', u'type': u'data', u'size': 426}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 490316, u'sha256': u'409664bc384377038c8e17156195a88f6819c0273530d451a3edbc0ebe4b9342', u'type': u'data', u'size': 396}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 490712, u'sha256':

u'0d10bf879173f9136af0bd077627063c43b2e5609b7bfba7f158544f4429e2e6', u'type': u'data', u'size': 300}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 491012, u'sha256': u'd7e5ec62539ece10aaf1e6edd0518577a5c47cd7b52a7bb62786f5cef00c9c53', u'type': u'data', u'size': 2510}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 493524, u'sha256': u'a6321dcf9148bfcf2d662f75bd02bb2635295f9ba77497dc73f624c13b60de96', u'type': u'data', u'size': 2736}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 496260, u'sha256': u'9c8e58b0377a3119f584fad973251238ce11076805af5039cadbf4640fe1ee0f', u'type': u'data', u'size': 2762}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 499024, u'sha256': u'ab464667e0e22d481aace9368936ac51945356f5f5fb93486c2eed7543dad4db', u'type': u'data', u'size': 2364}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 501388, u'sha256': u'4dc87da676ffc36c51be8e7320341562fc8f888dc30598365d675617d45bcc60', u'type': u'data', u'size': 1620}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 503008, u'sha256': u'a0c2f4fc5a466fda1a6c879e38e6a02c2679a166a855dff600d72cbb12353ef9', u'type': u'data', u'size': 1408}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 504416, u'sha256': u'a8efa60ba5b443fd8048fdd281285d54924802500ab1235a2c5b10a99034c920', u'type': u'data', u'size': 1422}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 505840, u'sha256': u'fe96257d65fa702aff1e703afd9dfe859b97d195898406ae4351ac4f27f1c7b4', u'type': u'data', u'size': 1488}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 507328, u'sha256': u'7ba9fe63361f241a3cf8caf3698f1fd903b3e937b325c8c995c3d93b4affbc9d', u'type': u'data', u'size': 2592}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 509920, u'sha256': u'e275a4adb04f89511ca5ff00b11cfa6148884382c2def8d93956ff4fb3175ee9', u'type': u'data', u'size': 940}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 510860, u'sha256': u'93f45374d169f3144568a8fc503e933842df0e4c60df1cf16aa8274ed1f29d2a', u'type': u'data', u'size': 336}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 511196, u'sha256': u'b29d7f3a4e66d5cc11d25538fccbdbea47f3bcddd5f5617d1efe097f62343e4c', u'type': u'data', u'size': 286}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 511484, u'sha256': u'4f6e434070d9e68aaccf5c49ca2d8ccc2a0d4669f280f9b307a82896b7226ad6', u'type': u'data', u'size': 326}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 511812, u'sha256': u'be18d8c081be944d61d27a48dcee6b9ec93070999d93ef1298f945919bd06560', u'type': u'data', u'size': 270}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 512084, u'sha256': u'1517597eae294617a5ce7b3ae21708f652659c4aefb70b494f7dde7e00236592', u'type': u'data', u'size': 194}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 512280, u'sha256': u'54e8194c123cb9c249a2e2f4a00a9f688fe77107b3729389a60f7f75e6fb9b45', u'type': u'data', u'size': 1852}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 514132, u'sha256': u'245733eceb7bf3399e2a873c74f50df0c9f1433a181cbc788fc29cf1b1606c0b', u'type': u'data', u'size': 1872}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 516004, u'sha256': u'2cf55e32d9d900a15a8d3d49c4d19bdc4367f574222ec627ee95737206fdb879', u'type': u'data', u'size': 1926}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 517932, u'sha256': u'bf19f78b7282e1497e7fe7d9abf281f34590eb70dc649c3dcd1c8c810b0a1864', u'type': u'data', u'size': 1432}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 519364, u'sha256': u'cc387194724963f52f9babdc60c5c183a6545b0edfc5d32296814197be797b64', u'type': u'data', u'size': 776}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 520140, u'sha256': u'1d076b95d42d95ca2b76268a2e4f105b47b2d421a7cebf64408a12db2f5617a7', u'type': u'data', u'size': 2632}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 522772, u'sha256': u'f128c4d2b371ee4f5af1f2cedc3b3cdda9f4dcc66d08a4199c92a71c6dd0d3b9', u'type': u'data', u'size': 2524}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 525296, u'sha256': u'95e9b90f848a44ed72d60fb3d6cfe6fb56392fb19419a6ec9cc9ece57fcded51', u'type': u'data', u'size': 2698}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 527996, u'sha256': u'2c3e28b5fbc013baa2ac4ed8d1982e20c1b24af439eaab4a619cc3e9ec203eca', u'type': u'data', u'size': 2012}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 530008, u'sha256': u'f2b8e8d9090ec83112a05b0dea5ee89145db19677acb90d0a5f8b87ed1f7d47c', u'type': u'data', u'size': 1268}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 531276, u'sha256': u'177584c46c7d734f33223e4c585ef9c97ca33a24e49c76b2f20f16964d531920', u'type': u'data', u'size': 56}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 531332, u'sha256': u'291b9c98b2aff4e003dcc57cf5a0a87eff44e0f7803a27282819d0ac6c3a93aa', u'type': u'data', u'size': 62}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 531396, u'sha256': u'66f1747ba4c17f6fca44818ed98445f01645651c120e72f558245e2df6949d35', u'type': u'data', u'size': 402}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 531800, u'sha256': u'0facb5a0cb3ce6df000a594ad8d6428040190be9aaa982716e0587eab374cac9', u'type': u'data', u'size': 906}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 532708, u'sha256': u'c054645d86387fd491743027e6c2284d6a7262f6aced9321cbc1465cef2b6b1f', u'type': u'data', u'size': 794}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 533504, u'sha256': u'c1bc5318a82ea1a180961804002685 1947f6aa5171d904a9e60966f4551ca1a3', u'type': u'data', u'size': 732}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 534236, u'sha256': u'1b8660b0c53b94f3e029de58e56d08c8097a080244e9dc65d4155a9b603820d8', u'type': u'data', u'size': 172}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 534408, u'sha256': u'36db380991291cac5c99e42332efda20210f63985544d95e8fa6ef85bf2bdf8e', u'type': u'data', u'size': 1220}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 535628, u'sha256': u'7f51554313c6765ba649783a942064cdfe6f5a70248a6f56840f71969f87ced0', u'type': u'data', u'size': 612}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 536240, u'sha256': u'1f1b61a7f04edc3691a6c9350132b09929d5bfa1c900f6ff500e55c5ebc63212', u'type': u'data', u'size': 66}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_MESSAGETABLE', u'offset': 536308, u'sha256': u'ef493afd7e7a330a21862c1623e75eab30b223bf04d434d0e4fe006a2d7faef6', u'type': u'data', u'size': 1720}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 538028, u'sha256': u'1ae3e871bb24efadc5c3ed9b87b902421883b191abb09c3d1033e38d9e538d4b', u'type': u'MS Windows cursor resource - 2 icons, 32x256, hotspot @1x1', u'size': 34}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 538064, u'sha256': u'effad6fefb36f30033a0d7771cc29e4ea5a1ac90f3fffc62ac7199523ab39775', u'type': u'MS Windows icon resource - 4 icons, 32x32, 16 colors', u'size': 62}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 538128, u'sha256': u'02e13e26f1814821a875054ac74d9a9718357d0495c69a6d7d44e97b75c5d61c', u'type': u'data', u'size': 828}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 538956, u'sha256': u'c0a151bb9256b246770200bab8aa5c2ee99d84b88dc58e26e396444b44ba231c', u'type': u'exported SGML document, ASCII text, with CRLF line terminators', u'size': 1211}
{u'lang': u'LANG_NEUTRAL', u'name': u'30', u'offset': 540168, u'sha256': u'1a12454cf61b47cb5b00ccd3b5a7e012a81d8225a894f9b73ea60335d6b9d5f1', u'type': u'data', u'size': 93}
{u'lang': u'LANG_NEUTRAL', u'name': u'30', u'offset': 540264, u'sha256': u'cf5260d05db04a6c040dd17131c2114fbafd19b16c2dc5f6803c86135a6f8d0a', u'type': u'data', u'size': 93}
{u'lang': u'LANG_NEUTRAL', u'name': u'30', u'offset': 540360, u'sha256': u'cf5260d05db04a6c040dd17131c2114fbafd19b16c2dc5f6803c86135a6f8d0a', u'type': u'data', u'size': 93}
{u'lang': u'LANG_NEUTRAL', u'name': u'30', u'offset': 540456, u'sha256': u'cf5260d05db04a6c040dd17131c2114fbafd19b16c2dc5f6803c86135a6f8d0a', u'type': u'data', u'size': 93}
{u'lang': u'LANG_NEUTRAL', u'name': u'31', u'offset': 540552, u'sha256': u'8855508aade16ec573d21e6a485dfd0a7624085c1a14b5ecdd6485de0c6839a4', u'type': u'data', u'size': 5}
{u'lang': u'LANG_NEUTRAL', u'name': u'31', u'offset': 540560, u'sha256': u'cd34bb9272642d7bda02bc2ac728a464d3b34440cd544e980f3ef6732ca66166', u'type': u'ASCII text, with no line terminators', u'size': 4}
{u'lang': u'LANG_NEUTRAL', u'name': u'31', u'offset': 540564, u'sha256': u'54fe3b5c81d139b25b18f56ba340b060e3a5b7f6eeb91a2806681fdb5bf4e2d9', u'type': u'ASCII text, with no line terminators', u'size': 4}
{u'lang': u'LANG_NEUTRAL', u'name': u'31', u'offset': 540568, u'sha256': u'54fe3b5c81d139b25b18f56ba340b060e3a5b7f6eeb91a2806681fdb5bf4e2d9', u'type': u'ASCII text, with no line terminators', u'size': 4}
{u'lang': u'LANG_NEUTRAL', u'name': u'31', u'offset': 540572, u'sha256': u'54fe3b5c81d139b25b18f56ba340b060e3a5b7f6eeb91a2806681fdb5bf4e2d9', u'type': u'ASCII text, with no line terminators', u'size': 4}
{u'lang': u'LANG_NEUTRAL', u'name': u'31', u'offset': 540576, u'sha256': u'54fe3b5c81d139b25b18f56ba340b060e3a5b7f6eeb91a2806681fdb5bf4e2d9', u'type': u'ASCII text, with no line terminators', u'size': 4}
{u'lang': u'LANG_GERMAN', u'name': u'32', u'offset': 540580, u'sha256': u'07da7ff93bee19ef556a6b07f421d792001dc91f6ddd6381914c9756c97db605', u'type': u'Rich Text Format data, version 1, ANSI', u'size': 48073}
{u'lang': u'LANG_SPANISH', u'name': u'32', u'offset': 588656, u'sha256': u'df9455a0d22d9d33b351428bdf812d7610ba4dd198950d53f4ec840863076032', u'type': u'Rich Text Format data, version 1, ANSI', u'size': 46159}
{u'lang': u'LANG_FRENCH', u'name': u'32', u'offset': 634816, u'sha256': u'a41ac4ca3657043577e80eff46c81999ce103e700aacf37443635c7903c01081', u'type': u'Rich Text Format data, version 1, ANSI', u'size': 50321}
{u'lang': u'LANG_ENGLISH', u'name': u'32', u'offset': 685140, u'sha256': u'f79bc6cee9db6f65bd4eee32a8346ad0d808ae5d73f2806604d68fd85418d104', u'type': u'Rich Text Format data, version 1, ANSI', u'size': 47734}
{u'lang': u'LANG_JAPANESE', u'name': u'32', u'offset': 732876, u'sha256': u'82f4f97e72d3b69733559907ac53794ecaccb4bb3d32b2c7d6899ad783d9f006', u'type': u'Rich Text Format data, version 1, ANSI', u'size': 123656}
{u'lang': u'LANG_NEUTRAL', u'name': u'33', u'offset': 856532, u'sha256': u'ad08c3f27b4ca38dc1d631eee4a0f80ccc2a883829d712c6db65a4ad3a2ea9f0', u'type': u'data', u'size': 1899}
{u'lang': u'LANG_NEUTRAL', u'name': u'34', u'offset': 858432, u'sha256': u'e54cd7e62ff58028b216d060bf782429fcffeba87456baff6c59579f3b18cec9', u'type': u'bzip2 compressed data, block size = 900k', u'size': 16064}
{u'lang': u'LANG_NEUTRAL', u'name': u'34', u'offset': 874496, u'sha256': u'3848d34eef49072a98cea24f78a4ef653e69c9dd67a73322d0e64431a8eb9353', u'type': u'bzip2 compressed data, block size = 900k', u'size': 18591}
{u'lang': u'LANG_NEUTRAL', u'name': u'34', u'offset': 893088, u'sha256': u'f57c701f8da5a3f48d1864d559c1a6a25ed62044fc536d3cefff33537ea57c99', u'type': u'bzip2 compressed data, block size = 900k', u'size': 5077}
{u'lang': u'LANG_NEUTRAL', u'name': u'34', u'offset': 898168, u'sha256': u'f9999fdca1ba1568a94926e4a6f612fba772c93c57b9dab45bd7abd7a3a44f90', u'type': u'bzip2 compressed data, block size = 900k', u'size': 3023}
{u'lang': u'LANG_NEUTRAL', u'name': u'34', u'offset': 901192, u'sha256': u'586a70136d95d303ee71b9a3df0067220ec2d4cf280dfff669a31805c85c1ce4', u'type': u'bzip2 compressed data, block size = 900k', u'size': 11764}
{u'lang': u'LANG_NEUTRAL', u'name': u'1024', u'offset': 912956, u'sha256': u'4fe703b9d23fa79e54cbf1a0048df015d2c3c108fa9add5042d806fac470fc9f', u'type': u'data', u'size': 598}

CERTIFICATE VALIDATION

- Success ✔

[+] Thawte Timestamping CA	
Status	NoError ✔
Start Date	1997-01-01 00:00:00
End Date	2020-12-31 23:59:59
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Key Identifier	null
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	null
Crl link	null
Key Usage	null
Extended Usage	null

[+] Symantec Time Stamping Services CA - G2	
Status	NoError ✔
Start Date	2012-12-21 00:00:00
End Date	2020-12-30 23:59:59
Sha256	0b44526ab89f4778858bf831045ec218d0d57734caa10208ea3d8c90c1043266
Serial	7E93EBFB7CC64E59EA4B9A77D406FC3B
Subject Key Identifier	5f 9a f5 6e 5c cc cc 74 9a d4 dd 7d ef 3f db ec 4c 80 2e dd
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	null
Crl link	http://crl.thawte.com/ThawteTimestampingCA.crl
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	{"Time Stamping (1.3.6.1.5.5.7.3.8)"}

[+] VeriSign Class 3 Public Primary Certification Authority - G5	
Status	NoError ✔
Start Date	2006-11-08 00:00:00
End Date	2036-07-16 23:59:59
Sha256	d0c133d98cabb2199501a761f5b8b9afd30d870477a534b41400a6dc57f5d64d
Serial	18DAD19E267DE8BB4A2158CDCC6B3B4A
Subject Key Identifier	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Issuer Name	VeriSign Class 3 Public Primary Certification Authority - G5
Issuer Key Identifier	null
Crl link	null
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	null

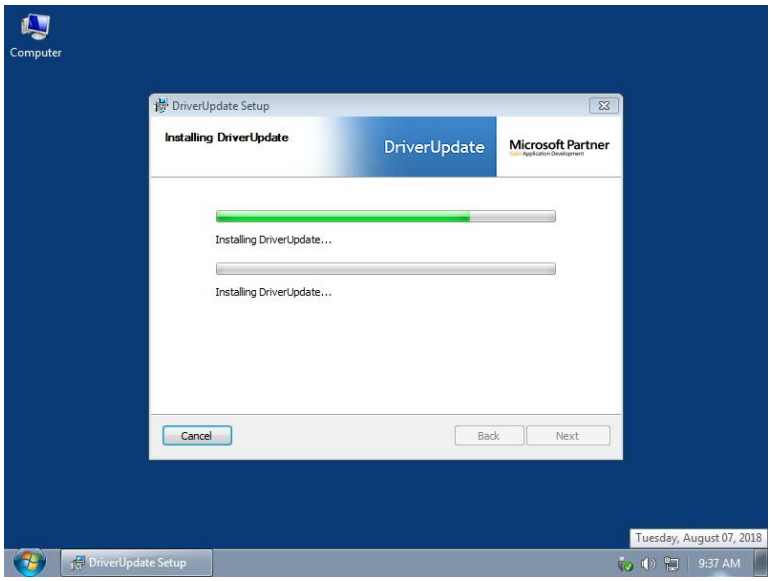
[+] VeriSign Class 3 Code Signing 2010 CA	
Status	NoError ✔
Start Date	2010-02-08 00:00:00
End Date	2020-02-07 23:59:59
Sha256	0f5cd6ebab15fa367e35893fad2bc49cd1a95449f58e7eb978d72bb0b100d764
Serial	5200E5AA2556FC1A86ED96C9D44B33C7
Subject Key Identifier	cf 99 a9 ea 7b 26 f4 4b c9 8e 8f d7 f0 05 26 ef e3 d2 a7 9d
Issuer Name	VeriSign Class 3 Public Primary Certification Authority - G5
Issuer Key Identifier	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Crl link	http://crl.verisign.com/pca3-g5.crl
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	{"Client Authentication (1.3.6.1.5.5.7.3.2)"}

[+] Slimware Utilities Holdings, Inc.	
Status	NoError ✔
Start Date	2015-02-23 00:00:00
End Date	2018-01-06 23:59:59
Sha256	bd240ba8dcfba6cd06ca1d93d971fe401656575461970d65099260ed3d4dbb8f
Serial	246BBE812B36C137225497BA8DF178FA
Subject Key Identifier	a6 c4 12 ae e2 9c a0 d5 9f 49 fe dd 22 89 dc 63 16 5f 42 38
Issuer Name	VeriSign Class 3 Code Signing 2010 CA
Issuer Key Identifier	cf 99 a9 ea 7b 26 f4 4b c9 8e 8f d7 f0 05 26 ef e3 d2 a7 9d
Crl link	http://sf.symcb.com/sf.crl
Key Usage	{"Digital Signature (80)"}
Extended Usage	{"Code Signing (1.3.6.1.5.5.7.3.3)"}

SCREENSHOTS

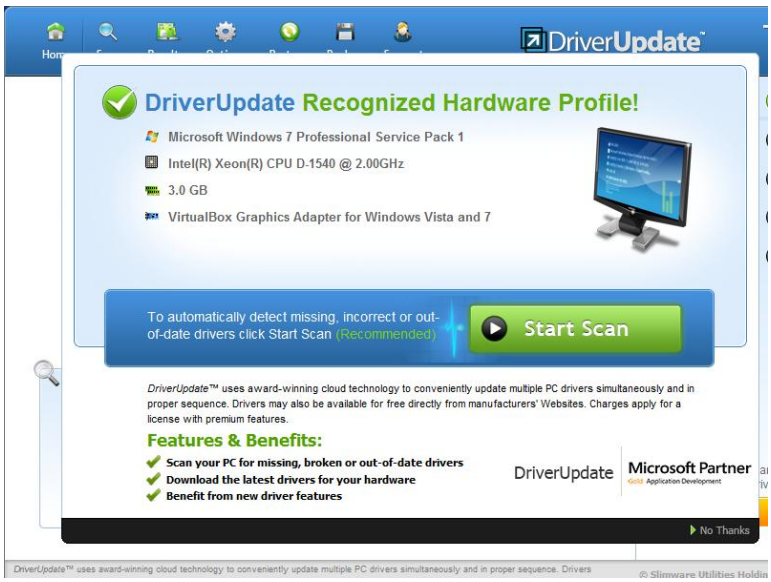

DriverUpdate
DriverUpdate Recognized Hardware Profile!
Microsoft Windows 7 Professional Service Pack 1
Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
3.0 GB
VirtualBox Graphics Adapter for Windows Vista and 7
To automatically detect missing, incorrect or out-of-date drivers click Start Scan (Recommended)
Start Scan
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers may also be available for free directly from manufacturers' Websites. Charges apply for a license with premium features.
Features & Benefits:
Scan your PC for missing, broken or out-of-date drivers
Download the latest drivers for your hardware
Benefit from new driver features
DriverUpdate
Microsoft Partner
No Thanks

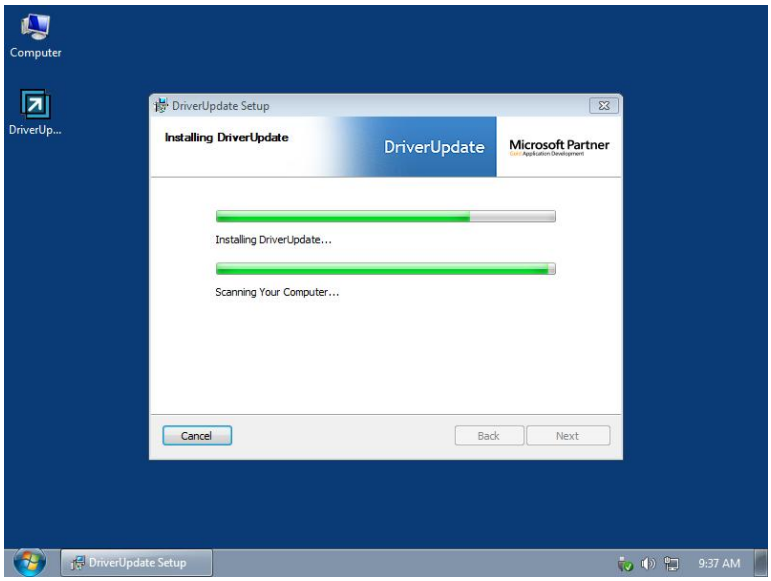

DriverUpdate
DriverUpdate Recognized Hardware Profile!
Microsoft Windows 7 Professional Service Pack 1
Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
3.0 GB
VirtualBox Graphics Adapter for Windows Vista and 7
To automatically detect missing, incorrect or out-of-date drivers click Start Scan (Recommended)
Start Scan
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers may also be available for free directly from manufacturers' Websites. Charges apply for a license with premium features.
Features & Benefits:
Scan your PC for missing, broken or out-of-date drivers
Download the latest drivers for your hardware
Benefit from new driver features
DriverUpdate
Microsoft Partner
No Thanks
DriverUpdate
9:40 AM

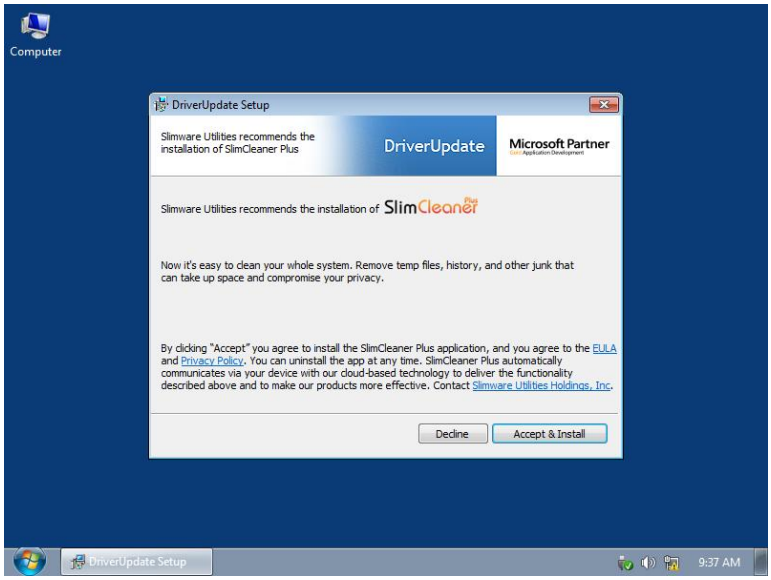

Computer
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Installing DriverUpdate...
Cancel
Back
Next
Tuesday, August 07, 2018
DriverUpdate Setup
9:37 AM

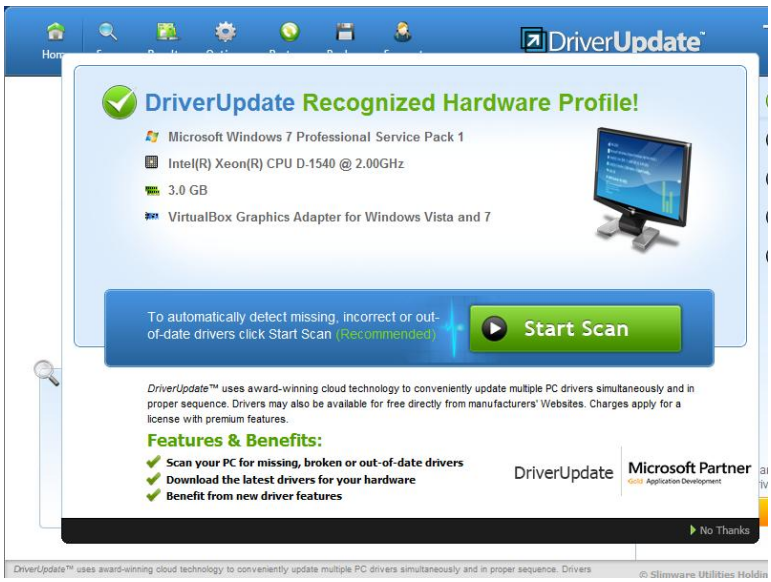

DriverUpdate
DriverUpdate Recognized Hardware Profile!
Microsoft Windows 7 Professional Service Pack 1
Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
3.0 GB
VirtualBox Graphics Adapter for Windows Vista and 7
To automatically detect missing, incorrect or out-of-date drivers click Start Scan (Recommended)
Start Scan
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers may also be available for free directly from manufacturers' Websites. Charges apply for a license with premium features.
Features & Benefits:
Scan your PC for missing, broken or out-of-date drivers
Download the latest drivers for your hardware
Benefit from new driver features
DriverUpdate
Microsoft Partner
No Thanks
DriverUpdate
9:40 AM

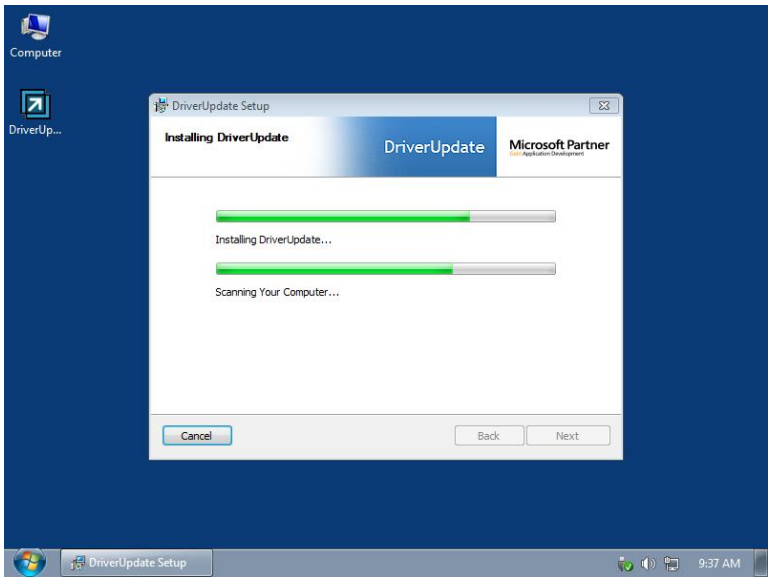

DriverUpdate
DriverUpdate Recognized Hardware Profile!
Microsoft Windows 7 Professional Service Pack 1
Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
3.0 GB
VirtualBox Graphics Adapter for Windows Vista and 7
To automatically detect missing, incorrect or out-of-date drivers click Start Scan (Recommended)
Start Scan
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers may also be available for free directly from manufacturers' Websites. Charges apply for a license with premium features.
Features & Benefits:
Scan your PC for missing, broken or out-of-date drivers
Download the latest drivers for your hardware
Benefit from new driver features
DriverUpdate
Microsoft Partner
No Thanks
DriverUpdate
9:39 AM


DriverUpdate
DriverUpdate Recognized Hardware Profile!
Microsoft Windows 7 Professional Service Pack 1
Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
3.0 GB
VirtualBox Graphics Adapter for Windows Vista and 7
To automatically detect missing, incorrect or out-of-date drivers click Start Scan (Recommended)
Start Scan
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers may also be available for free directly from manufacturers' Websites. Charges apply for a license with premium features.
Features & Benefits:
Scan your PC for missing, broken or out-of-date drivers
Download the latest drivers for your hardware
Benefit from new driver features
DriverUpdate
Microsoft Partner
No Thanks
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers


Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Scanning Your Computer...
Cancel
Back
Next
DriverUpdate Setup
9:37 AM

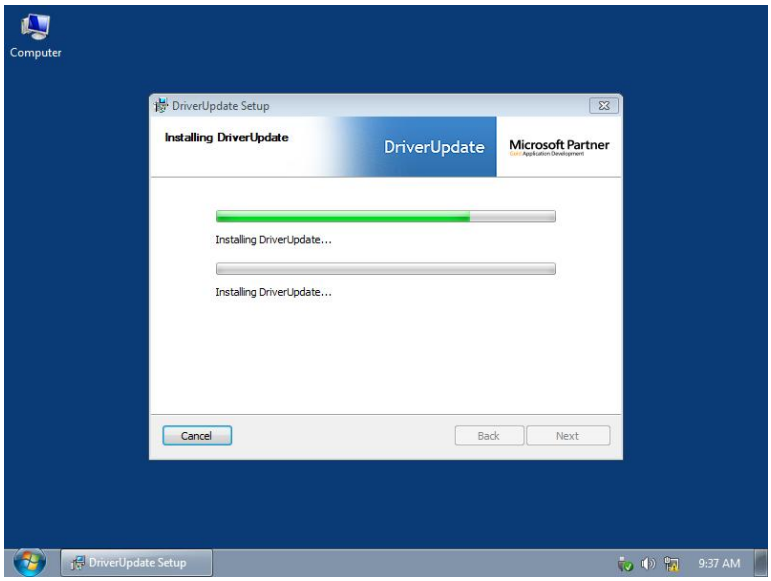

Computer
DriverUpdate Setup
Slimware Utilities recommends the installation of SlimCleaner Plus
DriverUpdate
Microsoft Partner
Slimware Utilities recommends the installation of SlimCleaner
Now it's easy to clean your whole system. Remove temp files, history, and other junk that can take up space and compromise your privacy.
By clicking "Accept" you agree to install the SlimCleaner Plus application, and you agree to the EULA and Privacy Policy. You can uninstall the app at any time. SlimCleaner Plus automatically communicates via your device with our cloud-based technology to deliver the functionality described above and to make our products more effective. Contact Slimware Utilities Holdings, Inc.
Decline
Accept & Install
DriverUpdate Setup
9:37 AM

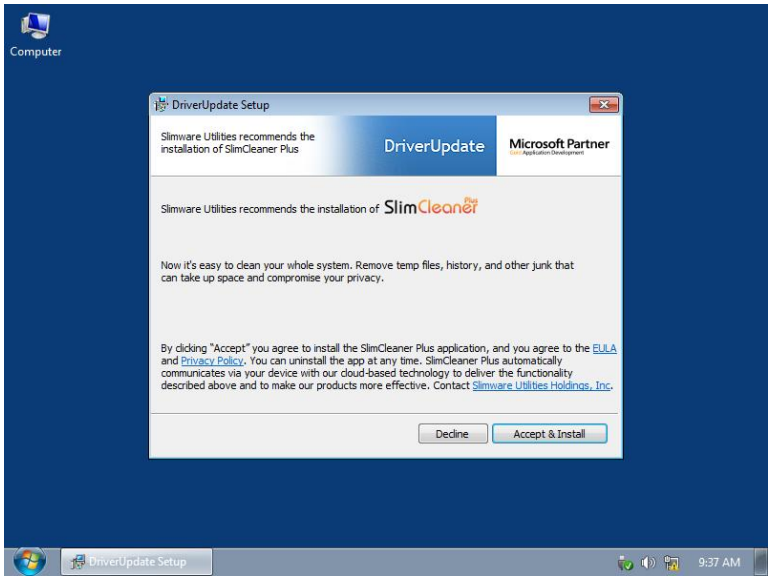

DriverUpdate
DriverUpdate Recognized Hardware Profile!
Microsoft Windows 7 Professional Service Pack 1
Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
3.0 GB
VirtualBox Graphics Adapter for Windows Vista and 7
To automatically detect missing, incorrect or out-of-date drivers click Start Scan (Recommended)
Start Scan
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers may also be available for free directly from manufacturers' Websites. Charges apply for a license with premium features.
Features & Benefits:
Scan your PC for missing, broken or out-of-date drivers
Download the latest drivers for your hardware
Benefit from new driver features
DriverUpdate
Microsoft Partner
No Thanks
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers


Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Scanning Your Computer...
Cancel
Back
Next
DriverUpdate Setup
9:37 AM


DriverUpdate
DriverUpdate Recognized Hardware Profile!
Microsoft Windows 7 Professional Service Pack 1
Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
3.0 GB
VirtualBox Graphics Adapter for Windows Vista and 7
To automatically detect missing, incorrect or out-of-date drivers click Start Scan (Recommended)
Start Scan
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers may also be available for free directly from manufacturers' Websites. Charges apply for a license with premium features.
Features & Benefits:
Scan your PC for missing, broken or out-of-date drivers
Download the latest drivers for your hardware
Benefit from new driver features
DriverUpdate
Microsoft Partner
No Thanks
DriverUpdate
9:39 AM


DriverUpdate
DriverUpdate Recognized Hardware Profile!
Microsoft Windows 7 Professional Service Pack 1
Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
3.0 GB
VirtualBox Graphics Adapter for Windows Vista and 7
To automatically detect missing, incorrect or out-of-date drivers click Start Scan (Recommended)
Start Scan
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers may also be available for free directly from manufacturers' Websites. Charges apply for a license with premium features.
Features & Benefits:
Scan your PC for missing, broken or out-of-date drivers
Download the latest drivers for your hardware
Benefit from new driver features
DriverUpdate
Microsoft Partner
No Thanks
DriverUpdate
9:39 AM

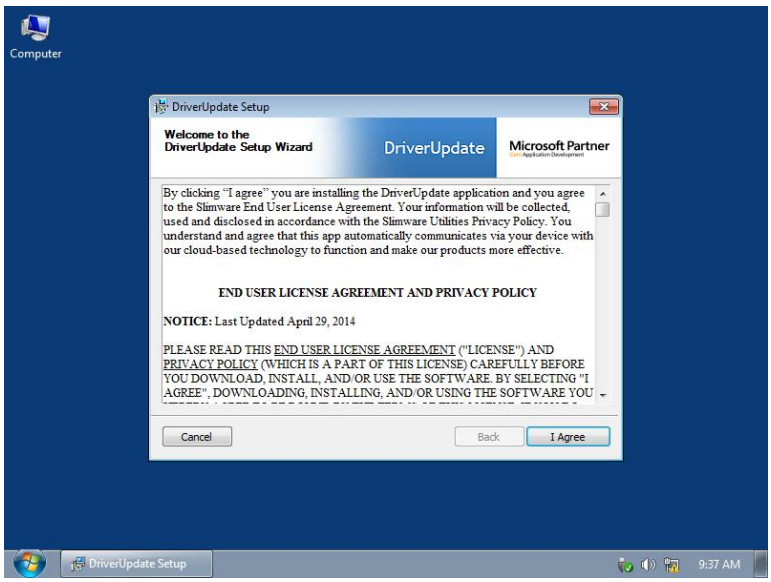

Computer
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Installing DriverUpdate...
Cancel
Back
Next
DriverUpdate Setup
9:37 AM


Computer
DriverUpdate Setup
Slimware Utilities recommends the installation of SlimCleaner Plus
DriverUpdate
Microsoft Partner
Slimware Utilities recommends the installation of SlimCleaner
Now it's easy to clean your whole system. Remove temp files, history, and other junk that can take up space and compromise your privacy.
By clicking "Accept" you agree to install the SlimCleaner Plus application, and you agree to the EULA and Privacy Policy. You can uninstall the app at any time. SlimCleaner Plus automatically communicates via your device with our cloud-based technology to deliver the functionality described above and to make our products more effective. Contact Slimware Utilities Holdings, Inc.
Decline
Accept & Install
DriverUpdate Setup
9:37 AM


Computer
DriverUp...
9:38 AM

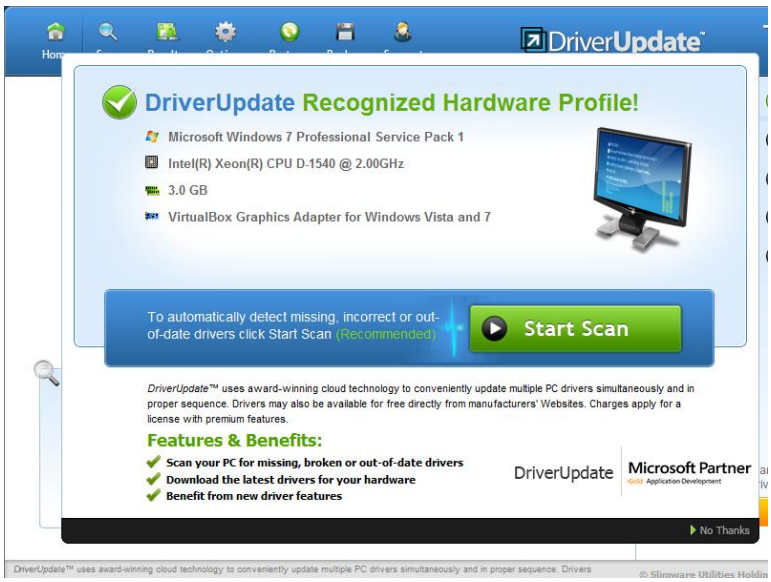

DriverUpdate
DriverUpdate Recognized Hardware Profile!
Microsoft Windows 7 Professional Service Pack 1
Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
3.0 GB
VirtualBox Graphics Adapter for Windows Vista and 7
To automatically detect missing, incorrect or out-of-date drivers click Start Scan (Recommended)
Start Scan
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers may also be available for free directly from manufacturers' Websites. Charges apply for a license with premium features.
Features & Benefits:
Scan your PC for missing, broken or out-of-date drivers
Download the latest drivers for your hardware
Benefit from new driver features
DriverUpdate
Microsoft Partner
No Thanks

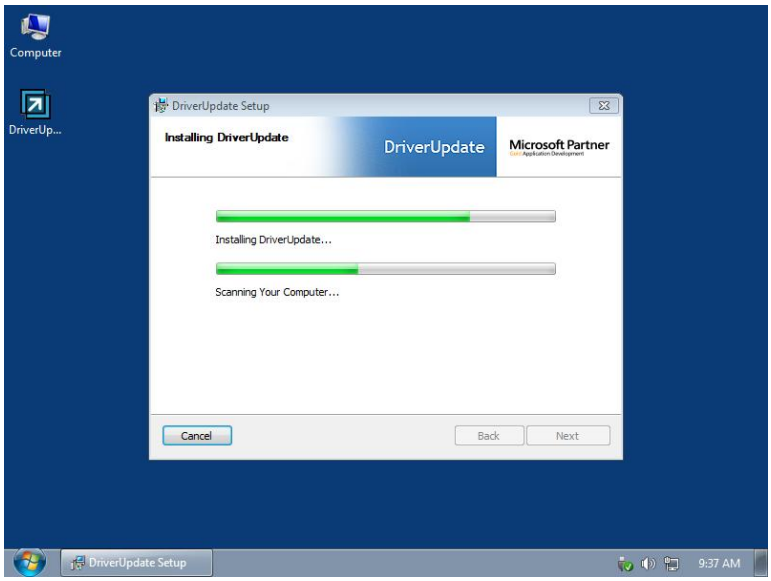

DriverUpdate
DriverUpdate Recognized Hardware Profile!
Microsoft Windows 7 Professional Service Pack 1
Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
3.0 GB
VirtualBox Graphics Adapter for Windows Vista and 7
To automatically detect missing, incorrect or out-of-date drivers click Start Scan (Recommended)
Start Scan
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers may also be available for free directly from manufacturers' Websites. Charges apply for a license with premium features.
Features & Benefits:
Scan your PC for missing, broken or out-of-date drivers
Download the latest drivers for your hardware
Benefit from new driver features
DriverUpdate
Microsoft Partner
No Thanks
DriverUpdate
9:39 AM

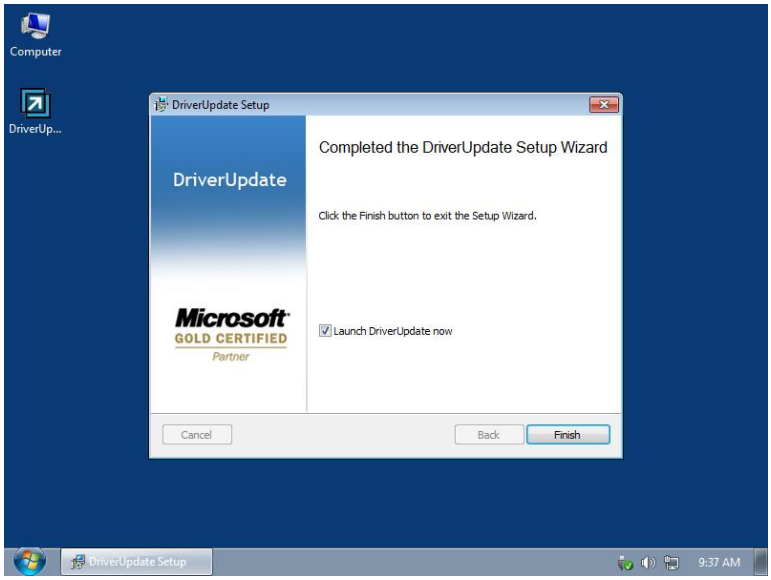

Computer
DriverUpdate Setup
Welcome to the DriverUpdate Setup Wizard
DriverUpdate
Microsoft Partner
By clicking "I agree" you are installing the DriverUpdate application and you agree to the Slimware End User License Agreement. Your information will be collected, used and disclosed in accordance with the Slimware Utilities Privacy Policy. You understand and agree that this app automatically communicates via your device with our cloud-based technology to function and make our products more effective.
END USER LICENSE AGREEMENT AND PRIVACY POLICY
NOTICE: Last Updated April 29, 2014
PLEASE READ THIS END USER LICENSE AGREEMENT ("LICENSE") AND PRIVACY POLICY (WHICH IS A PART OF THIS LICENSE) CAREFULLY BEFORE YOU DOWNLOAD, INSTALL, AND/OR USE THE SOFTWARE. BY SELECTING "I AGREE", DOWNLOADING, INSTALLING, AND/OR USING THE SOFTWARE YOU
Cancel
Back
I Agree
DriverUpdate Setup
9:37 AM

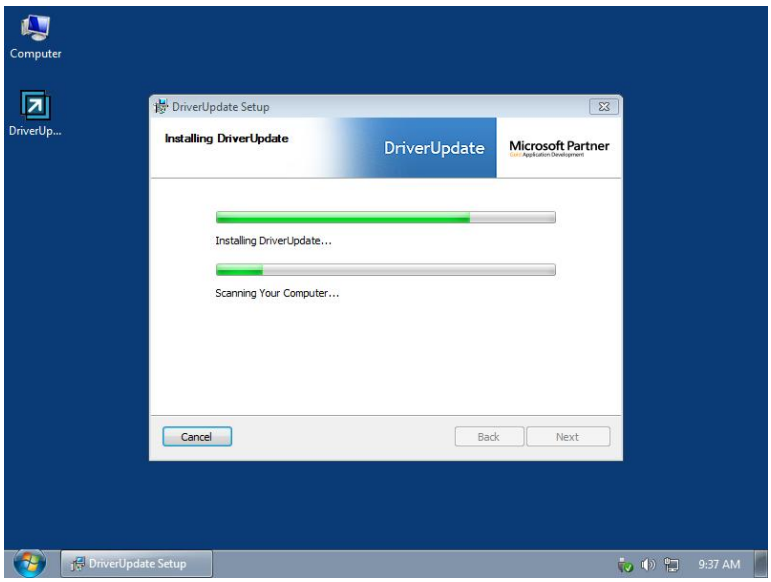

DriverUpdate
DriverUpdate Recognized Hardware Profile!
Microsoft Windows 7 Professional Service Pack 1
Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
3.0 GB
VirtualBox Graphics Adapter for Windows Vista and 7
To automatically detect missing, incorrect or out-of-date drivers click Start Scan (Recommended)
Start Scan
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers may also be available for free directly from manufacturers' Websites. Charges apply for a license with premium features.
Features & Benefits:
Scan your PC for missing, broken or out-of-date drivers
Download the latest drivers for your hardware
Benefit from new driver features
DriverUpdate
Microsoft Partner
No Thanks

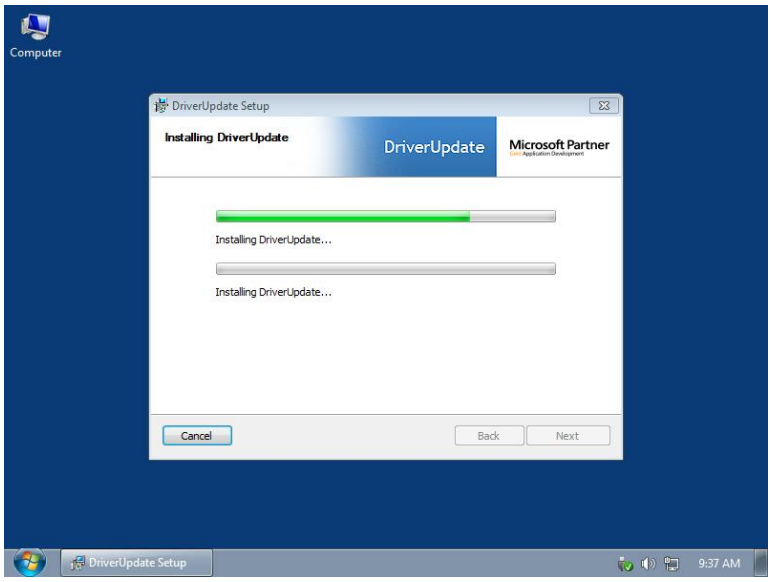

Computer
9:37 AM

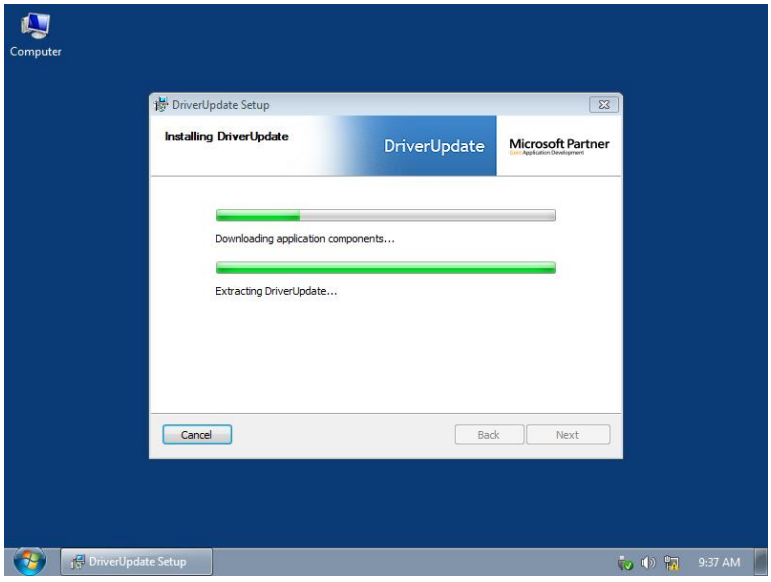

DriverUpdate
DriverUpdate Recognized Hardware Profile!
Microsoft Windows 7 Professional Service Pack 1
Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
3.0 GB
VirtualBox Graphics Adapter for Windows Vista and 7
To automatically detect missing, incorrect or out-of-date drivers click Start Scan (Recommended)
Start Scan
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers may also be available for free directly from manufacturers' Websites. Charges apply for a license with premium features.
Features & Benefits:
Scan your PC for missing, broken or out-of-date drivers
Download the latest drivers for your hardware
Benefit from new driver features
DriverUpdate
Microsoft Partner
No Thanks


Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Scanning Your Computer...
Cancel
Back
Next
DriverUpdate Setup
9:37 AM

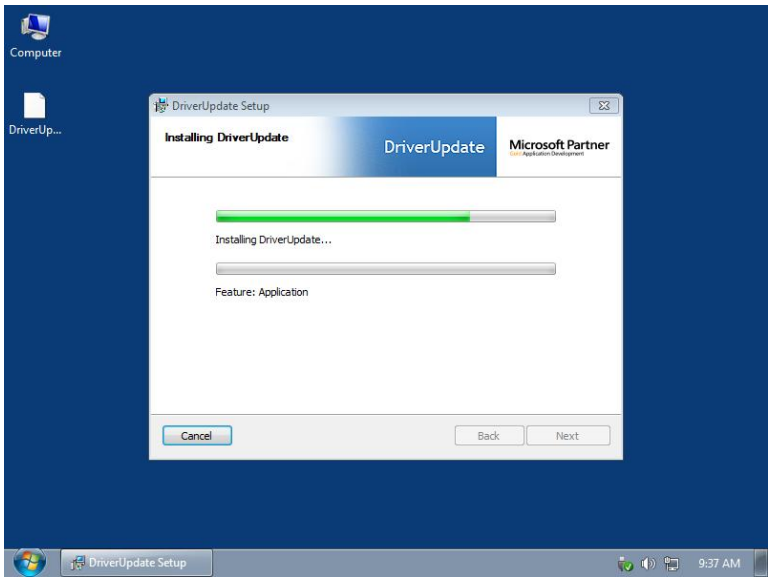

Computer
DriverUp...
DriverUpdate Setup
DriverUpdate
Completed the DriverUpdate Setup Wizard
Click the Finish button to exit the Setup Wizard.
Microsoft
GOLD CERTIFIED
Partner
Launch DriverUpdate now
Cancel
Back
Finish
DriverUpdate Setup
9:37 AM


Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Scanning Your Computer...
Cancel
Back
Next
DriverUpdate Setup
9:37 AM

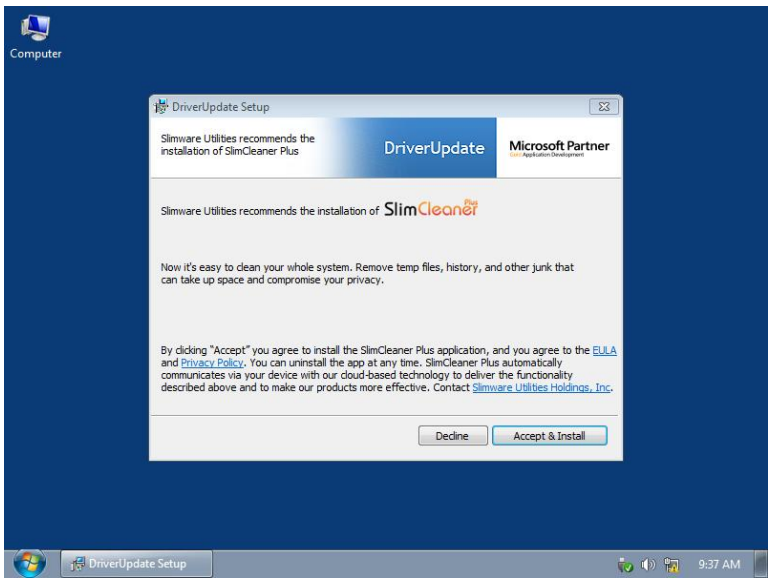

Computer
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Installing DriverUpdate...
Cancel
Back
Next
DriverUpdate Setup
9:37 AM


Computer
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Downloading application components...
Extracting DriverUpdate...
Cancel
Back
Next
DriverUpdate Setup
9:37 AM

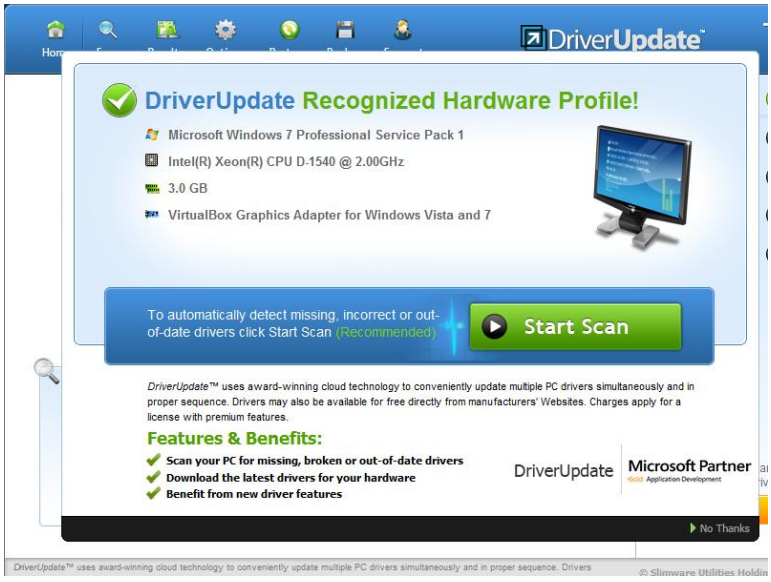

DriverUpdate
DriverUpdate Recognized Hardware Profile!
Microsoft Windows 7 Professional Service Pack 1
Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
3.0 GB
VirtualBox Graphics Adapter for Windows Vista and 7
To automatically detect missing, incorrect or out-of-date drivers click Start Scan (Recommended)
Start Scan
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers may also be available for free directly from manufacturers' Websites. Charges apply for a license with premium features.
Features & Benefits:
Scan your PC for missing, broken or out-of-date drivers
Download the latest drivers for your hardware
Benefit from new driver features
DriverUpdate
Microsoft Partner
No Thanks
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers


Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Feature: Application
Cancel
Back
Next
DriverUpdate Setup
9:37 AM


Computer
DriverUp...
SlimClea... Plus
9:38 AM


Computer
DriverUpdate Setup
Slimware Utilities recommends the installation of SlimCleaner Plus
DriverUpdate
Microsoft Partner
Slimware Utilities recommends the installation of SlimCleaner Plus
Now it's easy to clean your whole system. Remove temp files, history, and other junk that can take up space and compromise your privacy.
By clicking "Accept" you agree to install the SlimCleaner Plus application, and you agree to the EULA and Privacy Policy. You can uninstall the app at any time. SlimCleaner Plus automatically communicates via your device with our cloud-based technology to deliver the functionality described above and to make our products more effective. Contact Slimware Utilities Holdings, Inc.
Decline
Accept & Install
DriverUpdate Setup
9:37 AM


DriverUpdate
DriverUpdate Recognized Hardware Profile!
Microsoft Windows 7 Professional Service Pack 1
Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
3.0 GB
VirtualBox Graphics Adapter for Windows Vista and 7
To automatically detect missing, incorrect or out-of-date drivers click Start Scan (Recommended)
Start Scan
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers may also be available for free directly from manufacturers' Websites. Charges apply for a license with premium features.
Features & Benefits:
Scan your PC for missing, broken or out-of-date drivers
Download the latest drivers for your hardware
Benefit from new driver features
DriverUpdate
Microsoft Partner
No Thanks


DriverUpdate
DriverUpdate Recognized Hardware Profile!
Microsoft Windows 7 Professional Service Pack 1
Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
3.0 GB
VirtualBox Graphics Adapter for Windows Vista and 7
To automatically detect missing, incorrect or out-of-date drivers click Start Scan (Recommended)
Start Scan
DriverUpdate™ uses award-winning cloud technology to conveniently update multiple PC drivers simultaneously and in proper sequence. Drivers may also be available for free directly from manufacturers' Websites. Charges apply for a license with premium features.
Features & Benefits:
Scan your PC for missing, broken or out-of-date drivers
Download the latest drivers for your hardware
Benefit from new driver features
DriverUpdate
Microsoft Partner
No Thanks