VALKYRIE COMODO

Summary

File Name: None

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

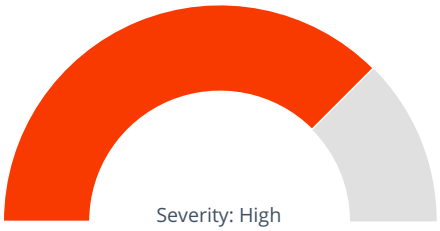
SHA1: 3776b000b8b93bee018a98b1338bac5b9eb18383

MD5:

MALWARE

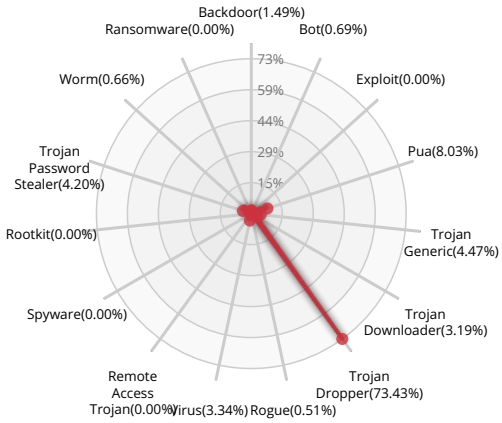
Valkyrie Final Verdict

DETECTION SECTION

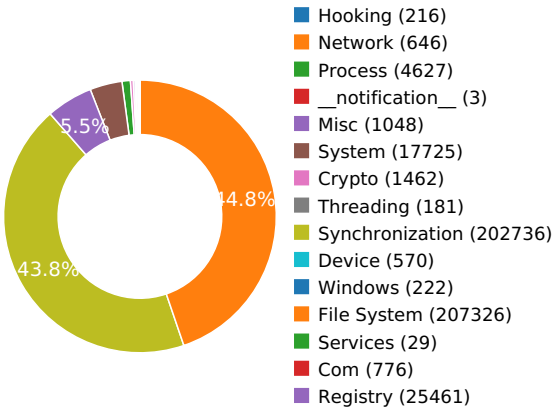


Verdict: Malware

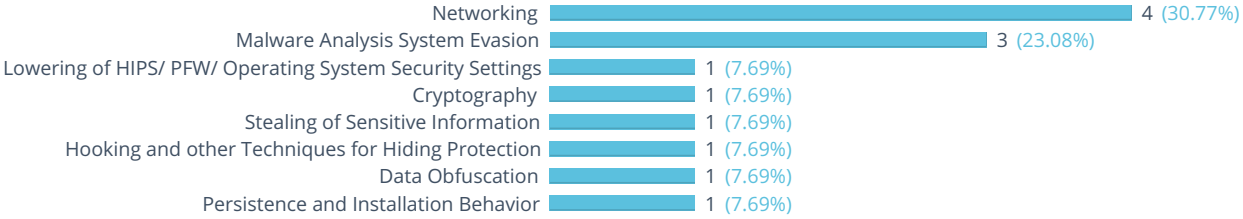
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

NETWORKING

Attempts to connect to a dead IP:Port (10 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

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys	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

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources

DATA OBFUSCATION

Drops a binary and executes it	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

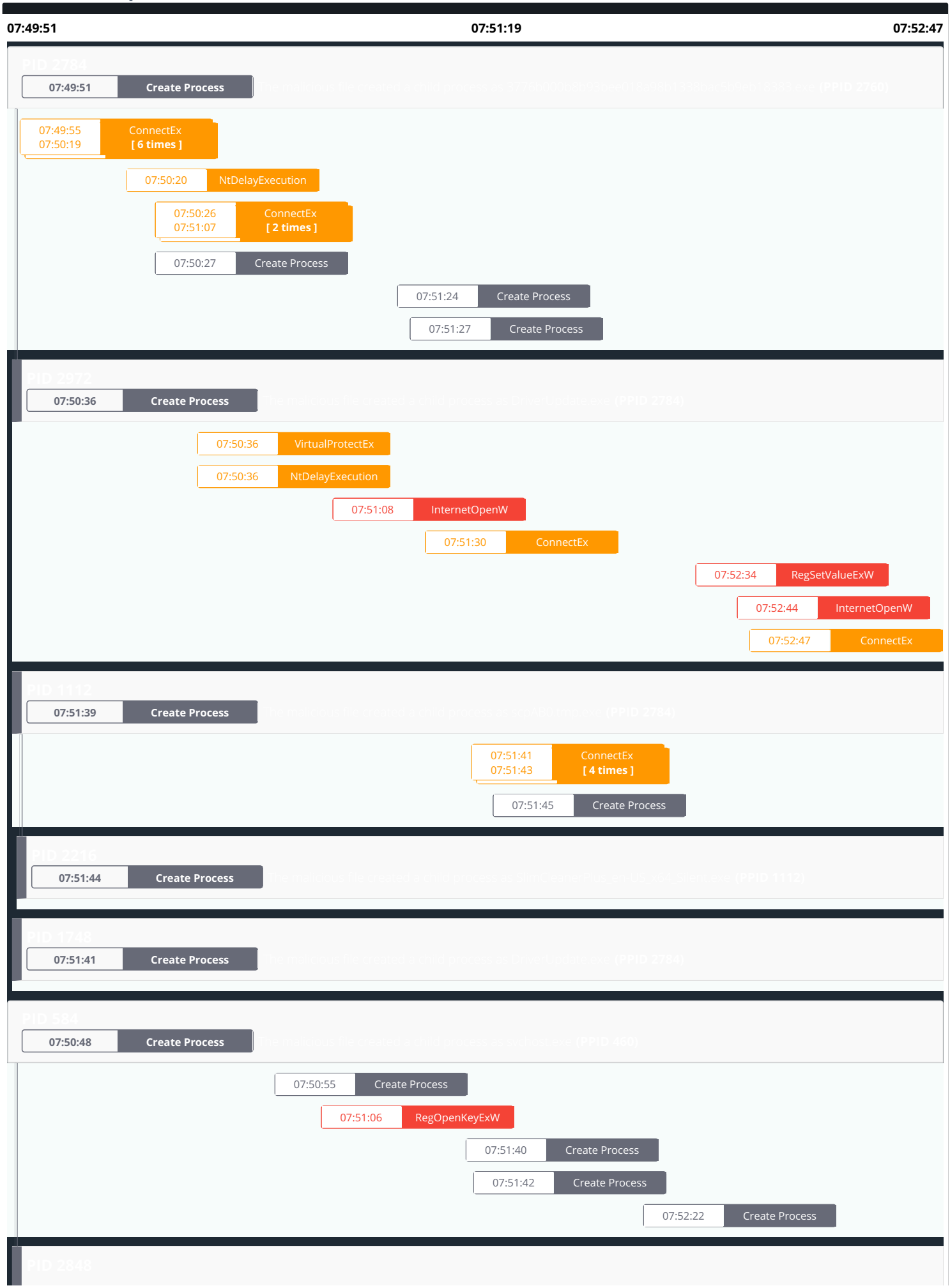
Installs itself for autorun at Windows startup	Show sources

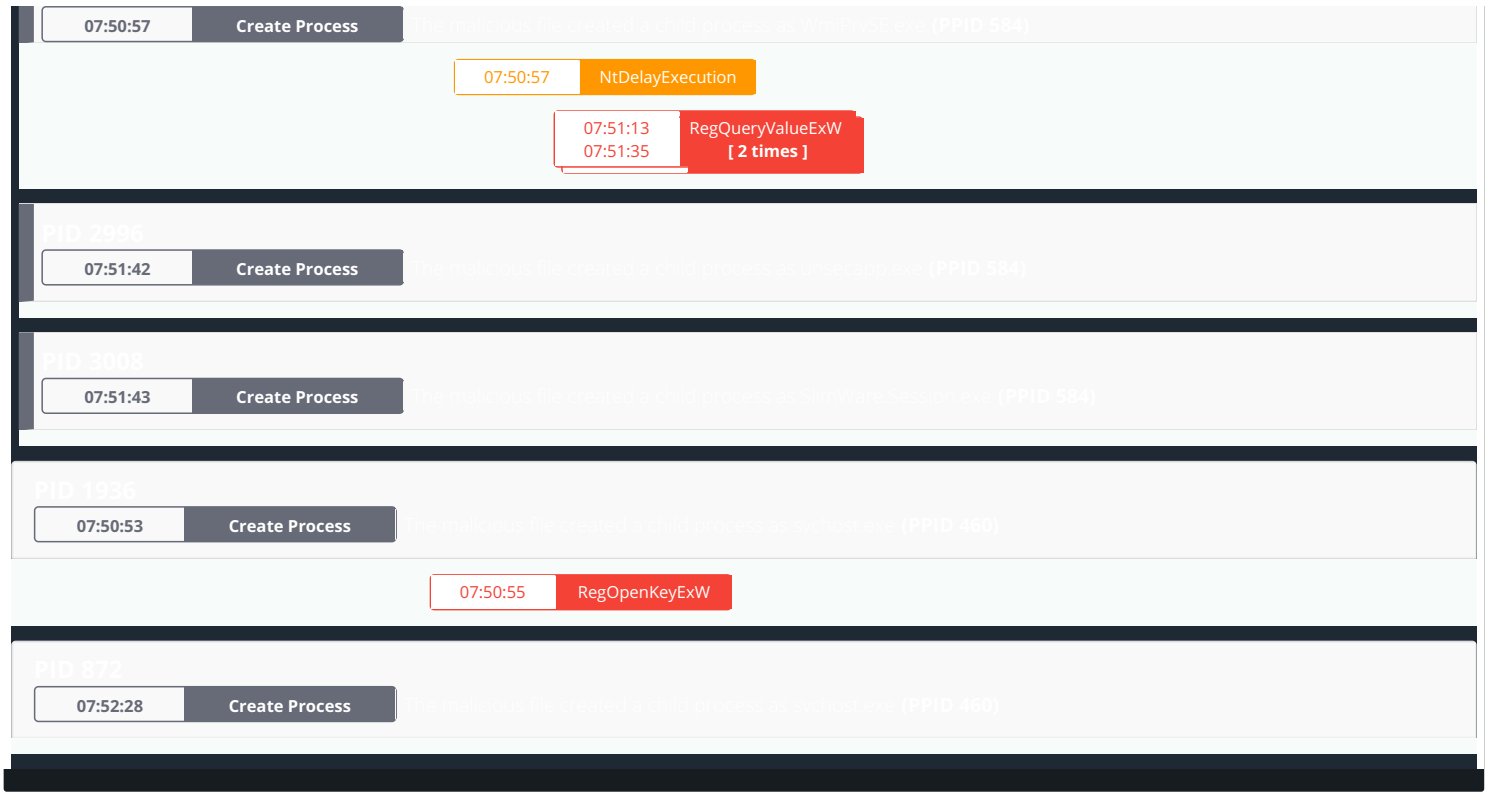
MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task.	Show sources
Detects VirtualBox through the presence of a registry key	Show sources
Checks the CPU name from registry, possibly for anti-virtualization	Show sources

VALKYRIE COMODO

Behavior Graph




07:50:57
Create Process
07:50:57
NtDelayExecution
07:51:13
07:51:35
RegQueryValueExW
[2 times]
PID 2996
07:51:42
Create Process
PID 3008
07:51:43
Create Process
PID 1936
07:50:53
Create Process
07:50:55
RegOpenKeyExW
PID 872
07:52:28
Create Process

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\3776b000b8b93bee018a98b1338bac5b9eb18383.exe.2.Manifest
C:\Users\user\AppData\Local\Temp\3776b000b8b93bee018a98b1338bac5b9eb18383.exe.3.Manifest
C:\Users\user\AppData\Local\Temp\3776b000b8b93bee018a98b1338bac5b9eb18383.exe.Config
C:\Users\user\AppData\Local\Temp\3776b000b8b93bee018a98b1338bac5b9eb18383.exe
C:\Users\user\AppData\Local\Temp\3776b000b8b93bee018a98b1338bac5b9eb18383.exe.installer_data
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\3776b000b8b93bee018a98b1338bac5b9eb18383.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\swuEFE3.tmp
C:\
C:\Users\user\AppData\Local\Temp\swuEFE3.tmp.msi
C:\Users\user\AppData\Local\Temp\scpAB0.tmp
C:\Users\user\AppData\Local\Temp\scpAB0.tmp.exe
C:\Windows\System32\p2pcollab.dll
C:\Windows\System32\qagentrt.dll
C:\Windows\System32\dnsapi.dll
C:\Windows\System32\en-US\DNSAPI.dll.mui
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates*
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
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\A092A81885DDD5AAD1EC1A803D7183779D81B6F9
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\BAED8A8C5A147CFA78E686BB4A8E5829C2F934F5
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\C8A51E044BF5AF39158BB24E414E8FDCD2891C3A
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\FB45378AB288E369B22C860D123A809F530D5CC1
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs*
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs*
C:\Windows\System32\en-US\WINHTTP.DLL.mui
C:\Users\user\AppData\LocalLow
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7D266D9E1E69FA1EEFB9699B009B34C8_*
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7D266D9E1E69FA1EEFB9699B009B34C8_0A9BFDD75B598C2110CBF610C078E6E6
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7D266D9E1E69FA1EEFB9699B009B34C8_0A9BFDD75B598C2110CBF610C078E6E6
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\9A19ADAD9D098E039450ABBEDD5616EB_*
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\9A19ADAD9D098E039450ABBEDD5616EB_04EB95CBF9CF5CBD7E29D6EC69DB8985
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\9A19ADAD9D098E039450ABBEDD5616EB_04EB95CBF9CF5CBD7E29D6EC69DB8985
C:\Program Files\DriverUpdate\DriverUpdate.exe
C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe
C:\Users\Public\Documents\Downloaded Installers
C:\Users\Public\Documents\Downloaded Installers\{EE6EFB90-09F2-4589-92FE-8B644AA35390}
C:\Users\Public\Documents\Downloaded Installers\{EE6EFB90-09F2-4589-92FE-8B644AA35390}\setup.msi
C:\Users\user\AppData\Local\Temp\
A:
B:
F:

G:
H:
I:
J:
K:
L:
M:
N:
O:

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
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\NET Framework Setup\NDP\v2.0.50727\Install
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v2.0.50727\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v3.0\Install
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v3.0\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v3.5\Install
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v3.5\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Install
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Client\Install
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Client\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Full\Install
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Full\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4.0\Install
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4.0\Client\Install
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4.0\Client\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Full\Release
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\OLE\MaximumAllowedAllocationSize
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\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

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\swuEFE3.tmp
C:\Users\user\AppData\Local\Temp\swuEFE3.tmp.msi
C:\Users\user\AppData\Local\Temp\scpAB0.tmp
C:\Users\user\AppData\Local\Temp\scpAB0.tmp.exe
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7D266D9E1E69FA1EEFB9699B009B34C8_0A9BFDD75B598C2110CBF610C078E6E6
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7D266D9E1E69FA1EEFB9699B009B34C8_0A9BFDD75B598C2110CBF610C078E6E6
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\9A19ADAD9D098E039450ABBEDD5616EB_04EB95CBF9CF5CBD7E29D6EC69DB8985
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\9A19ADAD9D098E039450ABBEDD5616EB_04EB95CBF9CF5CBD7E29D6EC69DB8985
C:\Users\Public\Documents\Downloaded Installers\{EE6EFB90-09F2-4589-92FE-8B644AA35390}\setup.msi
C:\Users\user\AppData\Local\Temp\MSIeece6.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\2018-08-19 10-14-56 0.log

C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Images\acer.png
C:\Windows\Tasks\DriverUpdate Scan.job
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Updates\hdd.exe
\??\PIPE\samr
C:\Windows\sysnative\wbem\repository\WRITABLE.TST
C:\Windows\sysnative\wbem\repository\MAPPING1.MAP
C:\Windows\sysnative\wbem\repository\MAPPING2.MAP
C:\Windows\sysnative\wbem\repository\MAPPING3.MAP
C:\Windows\sysnative\wbem\repository\OBJECTS.DATA
C:\Windows\sysnative\wbem\repository\INDEX.BTR
\??\pipe\PIPE_EVENTROOT\CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM
\??\WMIDataDevice
\??\PIPE\lsarpc
\??\PIPE\srvsvc
\??\PIPE\wkssvc
C:\Users\user\AppData\Local\Temp\SWI5D7D.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\Temp\SIOUT9346578\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\MSIeed3b.LOG
C:\Windows\sysnative\Tasks\DriverUpdate Scan

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
gdiplus.dll.GdiplusStartup
user32.dll.GetWindowInfo
user32.dll.GetAncestor
user32.dll.GetMonitorInfoA
user32.dll.EnumDisplayMonitors
user32.dll.EnumDisplayDevicesA
gdi32.dll.ExtTextOutW
gdi32.dll.GdiIsMetaPrintDC
ntdll.dll.RtlGetVersion
winhttp.dll.WinHttpGetIEProxyConfigForCurrentUser
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
iphlpapi.dll.ConvertInterfaceGuidToLuid
iphlpapi.dll.GetIfEntry2
iphlpapi.dll.GetIpForwardTable2
iphlpapi.dll.GetIpNetEntry2

DELETED FILES

C:\Users\user\AppData\Local\Temp\swuEFE3.tmp

C:\Users\user\AppData\Local\Temp\swuEFE3.tmp.msi
C:\Users\user\AppData\Local\Temp\scpAB0.tmp
C:\Users\user\AppData\Local\Temp\scpAB0.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:\Users\user\AppData\Local\Temp\SlimCleanerPlus_en-US_x64_Silent.exe
C:\Users\user\AppData\Local\Temp\SWI5D7D.tmp

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_CURRENT_USER\SOFTWARE\SlimWare Utilities Inc\LittleInstaller
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\NET Framework Setup\NDP
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v2.0.50727
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v2.0.50727\Install
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v2.0.50727\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v3.0
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v3.0\Install
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v3.0\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v3.5
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v3.5\Install
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v3.5\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Install
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Client
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Client\Install
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Client\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Full

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Full\Install
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Full\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4.0
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4.0\Install
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4.0\Client
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4.0\Client\Install
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4.0\Client\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Full\Release
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\3776b000b8b93bee018a98b1338bac5b9eb18383.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

EXECUTED COMMANDS

"C:\Program Files\DriverUpdate\DriverUpdate.exe" -installscan
"C:\Users\user\AppData\Local\Temp\scpAB0.tmp.exe" SI_LAUNCH=onreboot SI_MODE=toaster SI_DELAY=5 @P2_ORIGIN=^SW1^xdm111 @P2=^SW2^xdm059^^ @UL_STUBID=79a6e383-b52a-4838-ba5d-4bb20c9cf8b7
"C:\Program Files\DriverUpdate\DriverUpdate.exe" -installresults
C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
C:\Windows\system32\wbem\unsecapp.exe -Embedding
"C:\Program Files\SlimWare Utilities\Services\SlimWare.Session.exe" -Embedding
C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
"C:\Users\user\AppData\Local\Temp\SlimCleanerPlus_en-US_x64_Silent.exe" SI_LAUNCH=onreboot SI_MODE=toaster SI_DELAY=5

READ FILES

C:\Users\user\AppData\Local\Temp\3776b000b8b93bee018a98b1338bac5b9eb18383.exe.2.Manifest
C:\Users\user\AppData\Local\Temp\3776b000b8b93bee018a98b1338bac5b9eb18383.exe.3.Manifest
C:\Users\user\AppData\Local\Temp\3776b000b8b93bee018a98b1338bac5b9eb18383.exe.Config
C:\Users\user\AppData\Local\Temp\3776b000b8b93bee018a98b1338bac5b9eb18383.exe
C:\Users\user\AppData\Local\Temp\3776b000b8b93bee018a98b1338bac5b9eb18383.exe.installer_data
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\swuEFE3.tmp
C:\Users\user\AppData\Local\Temp\scpAB0.tmp
C:\Users\user\AppData\Local\Temp\swuEFE3.tmp.msi
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
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\A092A81885DDD5AAD1EC1A803D7183779D81B6F9
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\BAED8A8C5A147CFA78E686BB4A8E5829C2F934F5
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\C8A51E044BF5AF39158BB24E414E8FDCD2891C3A
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\FB45378AB288E369B22C860D123A809F530D5CC1
C:\Windows\System32\en-US\WINHTTP.DLL.mui
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7D266D9E1E69FA1EEFB9699B009B34C8_0A9BFDD75B598C2110CBF610C078E6E6
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7D266D9E1E69FA1EEFB9699B009B34C8_0A9BFDD75B598C2110CBF610C078E6E6
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\9A19ADAD9D098E039450ABBEDD5616EB_04EB95CBF9CF5CBD7E29D6EC69DB8985

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\9A19ADAD9D098E039450ABBEDD5616EB_04EB95CBF9CF5CBD7E29D6EC69DB8985
C:\Users\Public\Documents\Downloaded Installers\{EE6EFB90-09F2-4589-92FE-8B644AA35390}\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\DriverUpdate\DriverUpdate.exe.2.Manifest
C:\Program Files\DriverUpdate\DriverUpdate.exe.3.Manifest
C:\Program Files\DriverUpdate\DriverUpdate.exe.Config
C:\Program Files\DriverUpdate\DriverUpdate.exe
C:\Program Files\DriverUpdate\DriverUpdate.exe.1000.Manifest
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Windows\System32\en-US\dnsapi.DLL.mui
C:\Windows\System32\tzres.dll
C:\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\COMCTL32.dll.mui
C:\Windows\Tasks\DriverUpdate Scan.job
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Updates\hdd.exe
C:\Windows\sysnative\wbem\WmiPrvSE.exe
C:\Windows\inf\oem16.PNF
C:\Windows\sysnative\drivers\afd.sys
C:\Windows\sysnative\drivers\en-US\afd.sys.mui
C:\Windows\sysnative\tcpipcfg.dll
C:\Windows\sysnative\en-US\tcpipcfg.dll.mui
C:\Windows\sysnative\drivers\mountmgr.sys
C:\Windows\sysnative\drivers\en-US\mountmgr.sys.mui
C:\Windows\sysnative\FirewallAPI.dll
C:\Windows\sysnative\en-US\FirewallAPI.dll.mui
C:\Windows\sysnative\drivers\pacer.sys
C:\Windows\sysnative\drivers\en-US\pacer.sys.mui
C:\Windows\sysnative\clfs.sys
C:\Windows\sysnative\en-US\clfs.sys.mui
C:\Windows\sysnative\drivers\tssecsrv.sys
C:\Windows\sysnative\drivers\en-US\tssecsrv.sys.mui

MUTEXES

DBWinMutex
{042B0D65-EF5B-4E3F-ADFF-86C726E4F053}
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Global\MSILOG_25273f521d43778GOL.6eceeISM_pmeT_lacoL_ataDppA_resu_sresU_:C
Global_MSIExecute
SlimWare Utilities, Inc..DriverUpdate
IESQMMUTEX_0_208
Global\MSILOG_5c74730f1d43778GOL.b3deeISM_pmeT_lacoL_ataDppA_resu_sresU_:C

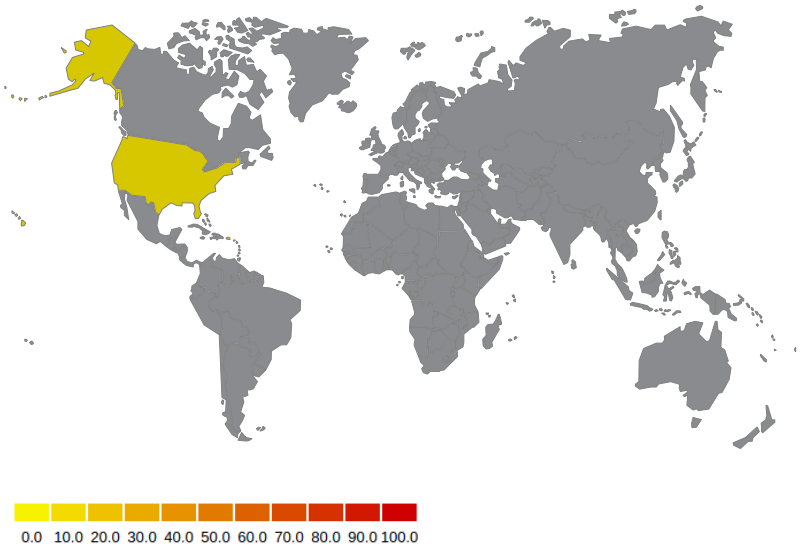
MODIFIED REGISTRY KEYS

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_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\GlobalAssocChangedCounter
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\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_CURRENT_USER\SOFTWARE\SlimWare Utilities Inc\DriverUpdate

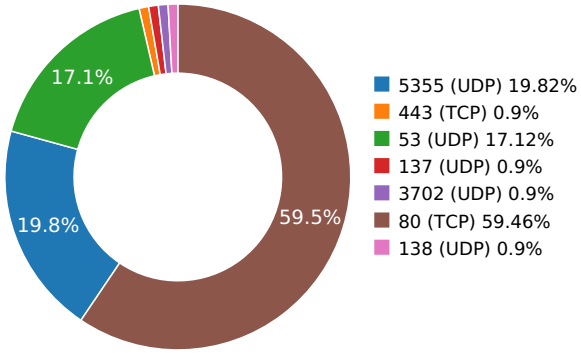
HKEY_CURRENT_USER\Software\SlimWare Utilities Inc\DriverUpdate\InstallScanUrlParams
HKEY_CURRENT_USER\Software\SlimWare Utilities Inc\DriverUpdate\InstallScanID
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6E\52C64B7E\LanguageList
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6E\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6E\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\DriverUpdate
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Transports\Decoupled\Server
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\CreationTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\MarshaledProxy
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\ProcessIdentifier
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ConfigValueEssNeedsLoading
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\List of event-active namespaces
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\ESS\//./root/CIMV2\SCM Event Provider
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\SlimCleaner Plus\Registration
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_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F722F65C-3BEA-45C3-9507-39418362A086}\Path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F722F65C-3BEA-45C3-9507-39418362A086}\Hash
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\DriverUpdate Scan\Id
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\DriverUpdate Scan\Index
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F722F65C-3BEA-45C3-9507-39418362A086}\Triggers
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F722F65C-3BEA-45C3-9507-39418362A086}\DynamicInfo
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\CurrentVersion\WindowsUpdate\Auto Update\AUOptions

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
	143.204.145.118	United States	16509	Amazon Technologies Inc.	Malware Process
	143.204.145.161	United States	16509	Amazon Technologies Inc.	Malware Process
	143.204.145.88	United States	16509	Amazon Technologies Inc.	Malware Process
	151.101.2.133	United States	54113	Fastly	Malware Process
	184.24.97.176	United States	20940	Akamai Technologies, Inc.	OS Process
	23.215.131.195	United States	20940	Akamai Technologies, Inc.	OS Process
	23.50.75.27	United States	3257	Akamai Technologies, Inc.	Malware Process
	34.226.146.234	United States	14618	Amazon Technologies Inc.	Malware Process
	34.231.33.210	United States	14618	Amazon Technologies Inc.	Malware Process
	52.2.26.10	United States	14618	Amazon Technologies Inc.	Malware Process
	54.175.217.102	United States	14618	Amazon Technologies Inc.	Malware Process
	54.209.147.46	United States	14618	Amazon Technologies Inc.	Malware Process
apps-api.slimwareutilities.com	52.44.174.33	United States	14618	Amazon Technologies Inc.	Malware Process
crl.microsoft.com	208.185.118.88	United States	6461	Not known	OS Process
cdn.slimcleaner.com	52.85.88.187	United States	16509	Amazon Technologies Inc.	Malware Process
driverrpc.driverupdate.net	52.205.82.36	United States	14618	Amazon Technologies Inc.	Malware Process
crl.globalsign.net	151.101.22.133	United States	54113	Fastly	Malware Process
sf.symcd.com	23.52.155.27	United States	1299	Akamai Technologies, Inc.	Malware Process
trk.slimwareutilities.com	52.54.9.186	United States	14618	Amazon Technologies Inc.	Malware Process
stc.slimwareutilities.com	52.55.74.238	United States	14618	Amazon Technologies Inc.	Malware Process
download.driverupdate.net	52.85.88.188	United States	16509	Amazon Technologies Inc.	Malware Process
ocsp.verisign.com	23.52.155.27	United States	1299	Akamai Technologies, Inc.	Malware Process

Name	IP	Country	ASN	ASN Name	Trigger Process Type
ctldl.windowsupdate.com	208.185.118.90	United States	6461	Zayo Bandwidth	OS Process
www.driverupdate.net	54.84.213.244	United States	14618	Amazon Technologies Inc.	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	9.48273682594
Path: /ulc.php? ev=InstallerInvoked&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&platformOSVersion=6.1&productVersion=2.9.4&msBclVersion=4.6.0 **URI:** http://trk.slimwareutilities.com/ulc.php? ev=InstallerInvoked&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&platformOSVersion=6.1&productVersion=2.9.4&msBclVersion=4.6.0						
download.driverupdate.net	80	GET	1.1	SLIMHTTP/1.1	1	9.9128370285
Path: /6.1/x64/DriverUpdate-setup.msi.bz2 **URI:** http://download.driverupdate.net/6.1/x64/DriverUpdate-setup.msi.bz2						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	10.905369997
Path: /ulc.php? ev=InstallerAccepted&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&platformOSVersion=6.1&productVersion=2.9.4 **URI:** http://trk.slimwareutilities.com/ulc.php? ev=InstallerAccepted&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&platformOSVersion=6.1&productVersion=2.9.4						
cdn.slimcleaner.com	80	GET	1.1	SLIMHTTP/1.1	1	16.8253920078
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	22.9505388737
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?c19dca041151c37e **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?c19dca041151c37e						
ocsp.verisign.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	28.5481920242
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	33.7817058563

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTSqZMG5M8TA9rdzkbCnNwuMAd5VgQUz5mp6nsm9EvJjo%2FX8AUm7%2BPSp50CECRrvoErNsE3IlSXuo3xePo%3D **URI:** http://sf.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTSqZMG5M8TA9rdzkbCnNwuMAd5VgQUz5mp6nsm9EvJjo%2FX8AUm7%2BPSp50CECRrvoErNsE3IlSXuo3xePo%3D						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	40.6423149109
Path: /ulc.php?ev=InstallerFinished&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi4wLjMyMDIuOTQiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&platformOSVersion=6.1&productVersion=2.9.4&installId=18F97E80-7D4A-4601-960B-A4A4A9414492 **URI:** http://trk.slimwareutilities.com/ulc.php?ev=InstallerFinished&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi4wLjMyMDIuOTQiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&platformOSVersion=6.1&productVersion=2.9.4&installId=18F97E80-7D4A-4601-960B-A4A4A9414492						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	43.2806208134
Path: /ulc.php?ev=TrackEvent&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi4wLjMyMDIuOTQiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&platformOSVersion=6.1&productVersion=2.9.4&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&description=InstallerScan-LI&result=installScanInitiated **URI:** http://trk.slimwareutilities.com/ulc.php?ev=TrackEvent&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi4wLjMyMDIuOTQiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&platformOSVersion=6.1&productVersion=2.9.4&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&description=InstallerScan-LI&result=installScanInitiated						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	70.3337898254
Path: /pki/crl/products/tspca.crl **URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	75.9558780193
Path: /pki/crl/products/CodeSignPCA2.crl **URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl						
apps-api.slimwareutilities.com	80	POST	1.1	PHP.Serialize	1	77.4907739162
Path: /v1/AutoActivate **URI:** http://apps-api.slimwareutilities.com/v1/AutoActivate						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	78.980629921
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	79.1531338692
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	81.0523808002

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /ulc.php?ev=Startup&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&hasUI=no&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi4wLjMyMDIuOTQiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&isRegistered=no&platformOS=Windows&eventSource=SYSTEM **URI:** http://trk.slimwareutilities.com/ulc.php?ev=Startup&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&hasUI=no&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi4wLjMyMDIuOTQiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&isRegistered=no&platformOS=Windows&eventSource=SYSTEM						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	81.1000418663
Path: /ulc.php?ev=TrackEvent&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&description=InstallerScan-DU&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi4wLjMyMDIuOTQiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&result=driverRPCRequestInitiated&platformOS=Windows **URI:** http://trk.slimwareutilities.com/ulc.php?ev=TrackEvent&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&description=InstallerScan-DU&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi4wLjMyMDIuOTQiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&result=driverRPCRequestInitiated&platformOS=Windows						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	81.4350249767
Path: /ulc.php?ev=TrackEvent&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi4wLjMyMDIuOTQiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&platformOSVersion=6.1&productVersion=2.9.4&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&description=InstallerScan-LI&result=installScanInProgress **URI:** http://trk.slimwareutilities.com/ulc.php?ev=TrackEvent&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi4wLjMyMDIuOTQiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&platformOSVersion=6.1&productVersion=2.9.4&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&description=InstallerScan-LI&result=installScanInProgress						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	97.6805980206
Path: /ulc.php?ev=TrackEvent&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&description=InstallerScan-DU&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi4wLjMyMDIuOTQiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&result=driverRPCRequestCompleted&platformOS=Windows **URI:** http://trk.slimwareutilities.com/ulc.php?ev=TrackEvent&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&description=InstallerScan-DU&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi4wLjMyMDIuOTQiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&result=driverRPCRequestCompleted&platformOS=Windows						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	97.9439308643

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /ulc.php? ev=TrackEvent&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&platformOSVersion=6.1&productVersion=2.9.4&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&description=InstallerScan-LI&result=installScanCompleted **URI:** http://trk.slimwareutilities.com/ulc.php? ev=TrackEvent&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&platformOSVersion=6.1&productVersion=2.9.4&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&description=InstallerScan-LI&result=installScanCompleted						
stc.slimwareutilities.com	80	GET	1.1	SilentDownloader/2.4.1	1	100.62590003
Path: /gettrack?product=SW1&p2=%5ESW2%5Exdm059%5E%5E&secondOfferOrigin=%5ESW1%5Exdm111&ul_stubid=79a6e383-b52a-4838-ba5d-4bb20c9cf8b7 **URI:** http://stc.slimwareutilities.com/gettrack?product=SW1&p2=%5ESW2%5Exdm059%5E%5E&secondOfferOrigin=%5ESW1%5Exdm111&ul_stubid=79a6e383-b52a-4838-ba5d-4bb20c9cf8b7						
cdn.slimcleaner.com	80	GET	1.1	SilentDownloader/2.4.1	1	101.004558802
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	101.13519001
Path: /ulc.php?ev=InstallerInvoked&platformOSVersion=6.1&secondOfferOrigin=%5ESW1%5Exdm111&ul_stubid=79a6e383-b52a-4838-ba5d-4bb20c9cf8b7&p2=%5ESW2%5Exdm059%5E%5E&installer=SD0&product=SW1&installerVersion=2.4.1&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&ul_track=SCP077 **URI:** http://trk.slimwareutilities.com/ulc.php?ev=InstallerInvoked&platformOSVersion=6.1&secondOfferOrigin=%5ESW1%5Exdm111&ul_stubid=79a6e383-b52a-4838-ba5d-4bb20c9cf8b7&p2=%5ESW2%5Exdm059%5E%5E&installer=SD0&product=SW1&installerVersion=2.4.1&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&ul_track=SCP077						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	101.56733799
Path: /ulc.php? ev=TrackEvent&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&platformOSVersion=6.1&productVersion=2.9.4&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&description=InstallerScan-LI&result=installResultsInitiated **URI:** http://trk.slimwareutilities.com/ulc.php? ev=TrackEvent&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&platformOSVersion=6.1&productVersion=2.9.4&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&description=InstallerScan-LI&result=installResultsInitiated						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	102.192683935
Path: /ulc.php? ev=InstallerFinishedButton&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&platformOSVersion=6.1&productVersion=2.9.4&installId=18F97E80-7D4A-4601-960B-A4A4A9414492 **URI:** http://trk.slimwareutilities.com/ulc.php? ev=InstallerFinishedButton&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&platformOSVersion=6.1&productVersion=2.9.4&installId=18F97E80-7D4A-4601-960B-A4A4A9414492						
sf.symcd.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	102.98186183

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTSqZMG5M8TA9rdzkbCnNwuMAd5VgQUz5mp6nsm9EvJjo%2FX8AUm7%2BPSp50CEDBjs6dAwc39%2BLuebDMa194%3D **URI:** http://sf.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTSqZMG5M8TA9rdzkbCnNwuMAd5VgQUz5mp6nsm9EvJjo%2FX8AUm7%2BPSp50CEDBjs6dAwc39%2BLuebDMa194%3D						
trk.slimwareutilities.com	80	GET	1.1	SilentDownloader/2.4.1	1	145.114710808
Path: /ulc.php?ev=InstallerFinished&platformOSVersion=6.1&secondOfferOrigin=%5ESW1%5Exdm111&installId=80F43C06-B396-40A9-9324-E5304CDE23EB&ul_stubid=79a6e383-b52a-4838-ba5d-4bb20c9cf8b7&p2=%5ESW2%5Exdm059%5E%5E&installer=SD0&product=SW1&installerVersion=2.4.1&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&ul_track=SCP077 **URI:** http://trk.slimwareutilities.com/ulc.php?ev=InstallerFinished&platformOSVersion=6.1&secondOfferOrigin=%5ESW1%5Exdm111&installId=80F43C06-B396-40A9-9324-E5304CDE23EB&ul_stubid=79a6e383-b52a-4838-ba5d-4bb20c9cf8b7&p2=%5ESW2%5Exdm059%5E%5E&installer=SD0&product=SW1&installerVersion=2.4.1&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows&ul_track=SCP077						
www.driverupdate.net	80	GET	1.1	DriverUpdate	1	159.790917873
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	159.866237879
Path: /images/test/acer.png **URI:** http://www.driverupdate.net/images/test/acer.png						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	3	168.307443857
Path: /ulc.php?ev=UIView&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&view=%2FMain%2FHome&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6lNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czoxMDoiZ2xvbiI7czozOiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows **URI:** http://trk.slimwareutilities.com/ulc.php?ev=UIView&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&view=%2FMain%2FHome&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6lNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czoxMDoiZ2xvbiI7czozOiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows						
apps-api.slimwareutilities.com	80	POST	1.1	DriverUpdate/5.1.1 (os:Win..	1	169.29539299
Path: /rpc/version-info **URI:** http://apps-api.slimwareutilities.com/rpc/version-info						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	169.610805988
Path: /ulc.php?ev=UIView&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&view=%2FConfirmAppUpdate&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6lNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czoxMDoiZ2xvbiI7czozOiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows **URI:** http://trk.slimwareutilities.com/ulc.php?ev=UIView&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&view=%2FConfirmAppUpdate&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6lNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czoxMDoiZ2xvbiI7czozOiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	172.77312398

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /ulc.php?ev=UIControl&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&owner=%2FConfirmAppUpdate&platformOS=Windows&label=Yes **URI:** http://trk.slimwareutilities.com/ulc.php?ev=UIControl&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&owner=%2FConfirmAppUpdate&platformOS=Windows&label=Yes						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	172.800084829
Path: /ulc.php?ev=UIView&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&view=%2FAppUpdateProgress&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows **URI:** http://trk.slimwareutilities.com/ulc.php?ev=UIView&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&view=%2FAppUpdateProgress&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	172.882211924
Path: /ulc.php?ev=TrackEvent&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&description=appUpdateDownloadInitiated&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows **URI:** http://trk.slimwareutilities.com/ulc.php?ev=TrackEvent&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&description=appUpdateDownloadInitiated&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows						
www.driverupdate.net	80	GET	1.1	DriverUpdate/5.1.1 (os:Win..	1	172.981850863
Path: /update.php?rpcvi=5.6.2%7C2018-06-01&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30= **URI:** http://www.driverupdate.net/update.php?rpcvi=5.6.2%7C2018-06-01&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiI2LjMiO30=						
www.driverupdate.net	80	GET	1.1	DriverUpdate/5.1.1 (os:Win..	4	173.06248188

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /update.php?rpcvi=5.6.2%7C2018-06-01&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czozOiI2LjMiO30= **URI:** http://www.driverupdate.net/update.php?rpcvi=5.6.2%7C2018-06-01&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czozOiI2LjMiO30=						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	173.415285826
Path: /ulc.php?ev=Error&page=appUpdateDownloadInitiated&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&errorType=windowsDesktopError&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czozOiI2LjMiO30%3D&errorCode=8007000E&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows **URI:** http://trk.slimwareutilities.com/ulc.php?ev=Error&page=appUpdateDownloadInitiated&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&errorType=windowsDesktopError&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czozOiI2LjMiO30%3D&errorCode=8007000E&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	173.483798027
Path: /ulc.php?ev=Error&page=appUpdateDownloadCompleted&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&errorType=windowsDesktopError&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czozOiI2LjMiO30%3D&errorCode=80070057&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows **URI:** http://trk.slimwareutilities.com/ulc.php?ev=Error&page=appUpdateDownloadCompleted&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&errorType=windowsDesktopError&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czozOiI2LjMiO30%3D&errorCode=80070057&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	173.518666983
Path: /ulc.php?ev=UIControl&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czozOiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&owner=%2FAppUpdateProgress&platformOS=Windows&label=Abort **URI:** http://trk.slimwareutilities.com/ulc.php?ev=UIControl&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czozOiI2LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&owner=%2FAppUpdateProgress&platformOS=Windows&label=Abort						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	173.546011925

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /ulc.php?ev=UIView&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&view=%2FAppUpdateDownloadFailed&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOjJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czoxMDoiV2luZG93czEwIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi42LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows **URI:** http://trk.slimwareutilities.com/ulc.php?ev=UIView&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&view=%2FAppUpdateDownloadFailed&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOjJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czoxMDoiV2luZG93czEwIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi42LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	174.950529814
Path: /ulc.php?ev=UIControl&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czoxMDoiV2luZG93czEwIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi42LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&owner=%2FAppUpdateDownloadFailed&platformOS=Windows&label=OK **URI:** http://trk.slimwareutilities.com/ulc.php?ev=UIControl&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czoxMDoiV2luZG93czEwIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi42LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&owner=%2FAppUpdateDownloadFailed&platformOS=Windows&label=OK						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	176.896477938
Path: /ulc.php?ev=Shutdown&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czoxMDoiV2luZG93czEwIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi42LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows **URI:** http://trk.slimwareutilities.com/ulc.php?ev=Shutdown&platformOSVersion=6.1&installId=18F97E80-7D4A-4601-960B-A4A4A9414492&browser=chrome&productVersion=5.1.1&product=SW2&sessionid=0A5F1DC6-1B4E-41DA-B166-045F9EE402B1&upl=YTo5OntzOjk6InVsX3N0dWJpZCI7czozNjoiNzlhNmUzODMtYjUyYS00ODM4LWJhNWQtNGJiMjBjOWNmOGI3IjtzOjEwOiJ1bF9jb2JyYW5kIjtzOjM6IlNXMiI7czoxMToidWxfY2FtcGFpZ24iO3M6NjoieGRtMDU5IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjExOiJicm93c2VyVHlwZSI7czo2OiJDaHJvbWUiO3M6MTQ6ImJyb3dzZXJWZXJzaW9uIjtzOjEyOiI2Mi4wLjMyMDIuOTQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czoxMDoiV2luZG93czEwIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czoiMi42LjMiO30%3D&machineId=2627B7B6-354E-493F-A8EB-2BD4E69565B7&platformOS=Windows						

DNS QUERIES

Request	Type
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 - 143.204.145.63 (A) - 143.204.145.88 (A) - 143.204.145.181 (A) - 143.204.145.18 (A)	
cdn.slimcleaner.com	A

Request	Type
Answers - 143.204.145.191 (A) - 143.204.145.161 (A) - 143.204.145.118 (A) - 143.204.145.39 (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) - 23.50.75.27 (A)	
sf.symcd.com	A
crl.microsoft.com	A
Answers - crl.www.ms.akadns.net (CNAME) - 23.215.131.200 (A) - 23.215.131.195 (A) - a1363.dscg.akamai.net (CNAME)	
apps-api.slimwareutilities.com	A
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.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.driverupdate.net	A
Answers - 52.205.82.36 (A) - 34.203.173.105 (A) - driver-rpc-2017-12-15-539119301.us-east-1.elb.amazonaws.com (CNAME) - 52.0.181.115 (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)	

Request	Type
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
9.48273682594	Sandbox	34.231.33.210	80
9.9128370285	Sandbox	143.204.145.88	80
16.8253920078	Sandbox	143.204.145.161	80
22.9505388737	Sandbox	184.24.97.176	80
28.5481920242	Sandbox	23.50.75.27	80
33.7817058563	Sandbox	23.50.75.27	80
40.6423149109	Sandbox	54.175.217.102	80
70.3337898254	Sandbox	23.215.131.195	80
77.4907739162	Sandbox	52.2.26.10	80
79.1531338692	Sandbox	151.101.2.133	80
81.0523808002	Sandbox	34.231.33.210	80
81.4350249767	Sandbox	34.231.33.210	80
95.7384409904	Sandbox	52.205.82.36	443
100.62590003	Sandbox	54.209.147.46	80
101.004558802	Sandbox	143.204.145.118	80
101.13519001	Sandbox	34.231.33.210	80
102.98186183	Sandbox	23.50.75.27	80
159.790917873	Sandbox	34.226.146.234	80
168.307443857	Sandbox	54.175.217.102	80
169.29539299	Sandbox	52.2.26.10	80
172.981850863	Sandbox	34.226.146.234	80
173.06248188	Sandbox	34.226.146.234	80
173.141357899	Sandbox	34.226.146.234	80
173.226161003	Sandbox	34.226.146.234	80
173.304306984	Sandbox	34.226.146.234	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.20859503746	Sandbox	224.0.0.252	5355

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.26372694969	Sandbox	224.0.0.252	5355
3.26491785049	Sandbox	192.168.56.255	137
3.27126598358	Sandbox	239.255.255.250	3702
5.81212091446	Sandbox	224.0.0.252	5355
6.84034585953	Sandbox	224.0.0.252	5355
7.28268098831	Sandbox	224.0.0.252	5355
8.34399986267	Sandbox	224.0.0.252	5355
9.26499891281	Sandbox	192.168.56.255	138
9.40716481209	Sandbox	8.8.4.4	53
9.84359383583	Sandbox	8.8.4.4	53
14.1397869587	Sandbox	224.0.0.252	5355
16.7031049728	Sandbox	8.8.4.4	53
17.6500179768	Sandbox	224.0.0.252	5355
20.2395839691	Sandbox	224.0.0.252	5355
22.7977240086	Sandbox	8.8.4.4	53
23.321295023	Sandbox	224.0.0.252	5355
25.8867828846	Sandbox	224.0.0.252	5355
28.4365408421	Sandbox	8.8.4.4	53
28.6096420288	Sandbox	224.0.0.252	5355
31.1853768826	Sandbox	224.0.0.252	5355
33.7345118523	Sandbox	8.8.4.4	53
38.0151100159	Sandbox	224.0.0.252	5355
40.5942399502	Sandbox	8.8.4.4	53
40.7120509148	Sandbox	224.0.0.252	5355
64.8099930286	Sandbox	224.0.0.252	5355
67.5431330204	Sandbox	224.0.0.252	5355
70.1963839531	Sandbox	8.8.4.4	53
70.4548449516	Sandbox	224.0.0.252	5355
73.3787069321	Sandbox	224.0.0.252	5355
74.6479918957	Sandbox	224.0.0.252	5355
76.2480559349	Sandbox	224.0.0.252	5355
77.4373049736	Sandbox	8.8.4.4	53
78.0696568489	Sandbox	224.0.0.252	5355
79.1060910225	Sandbox	8.8.4.4	53
80.8499479294	Sandbox	8.8.4.4	53
95.6042518616	Sandbox	8.8.4.4	53
99.7663710117	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
100.934162855	Sandbox	8.8.4.4	53
100.993532896	Sandbox	8.8.4.4	53
102.934625864	Sandbox	8.8.4.4	53
159.720858812	Sandbox	8.8.4.4	53
168.195034027	Sandbox	8.8.4.4	53
169.201613903	Sandbox	8.8.4.4	53

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 9db5db76c27c1f7dcc849db55a7e5c17 **SHA-1 :** b10d4d41d96dc70c9c3cb89bc8bba1eef4e8dcf8 **SHA-256 :** bd2ef8cde4b907536feba17d7e706a97314b063c **SHA-512 :** c64a64fb9631913982a85640c68f7af0b73b2d46f **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\Temp\SwuEFE3.Tmp.Msi **C:\Users\Public\Documents\Downloaded Installers\{EE6EFB90-09F2-4589-92FE-8B644AA35390}\Setup.Msi**	**Type :** Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, 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: x64;1033, Revision Number: {C1A9521B-EA12-4876-9C9D-876832C88EA9}, Create Time/Date: Mon Nov 13 19:40:52 2017, Last Saved Time/Date: Mon Nov 13 19:40:52 2017, Number of Pages: 200, Number of Words: 2, Name of Creating Application: Windows Installer XML Toolset (3.11.0.1701), Security: 2 **MD5 :** bd0ad961514a0684c40d0799d8b33713 **SHA-1 :** f292b0704e0e7918fff99d905d8ab4ea2c4d8ca6 **SHA-256 :** d13866ae3adfe8519890bb84870cb7a870cd10a8 **SHA-512 :** 016030810a489d532c3a1f5686de79528b66d898 **Size :** 45973.504 Kilobytes.
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 :** 8e0dbc8856a5c3fa95eea1ea95dc0072 **SHA-1 :** 85cb202b23ee15fc5bf83a6e45f63fec4a0e04ea **SHA-256 :** b18f4966ac8956f7f62781e97de6f4f5280ab6b44 **SHA-512 :** 4fed3a0b296001f5dbcb094868bcfdd4b67ccda7a **Size :** 0.512 Kilobytes.
C:\Users\User\AppData\Local\Temp\ScpAB0.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\Temp\SlimCleanerPlus_en-US_x64_Silent.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 075a229499b5ceaa0f439d4a5f01ff08 **SHA-1 :** 91c5827500b047ef80fa23347d02bdc56e0bab22 **SHA-256 :** e9caeed965005ceee2c1e3284af4201b95c8f66d2 **SHA-512 :** a79c8e39cae531a8f4fb653239bedcdec282309ef **Size :** 18697.568 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** Microsoft Cabinet archive data, 6509 bytes, 1 file **MD5 :** 33b39e2a516ef730a8fa922894f0fbd5 **SHA-1 :** 03d455583dda59215d945af76af6293b202f586f **SHA-256 :** 9446e8f2056fea3ac1365a809ada04602606242c3 **SHA-512 :** 75763aa13b43eb96294b0f84e131066111988726 **Size :** 6.509 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 26fd1bcf2dd2b99f929256eaf1a00e06 **SHA-1 :** 4d0e685ef7c593eb89d763e640cb2225c4dbfbdd **SHA-256 :** 7f0ea7c7bb432339f730c8b7a3c8e62dd5086741 **SHA-512 :** 01b42c3f8a1b0373f280595b1e0b49d20c45e60b **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\9A19ADAD9D098E039450ABBEDD5616EB_90968CAB679DC8A66D51322A089E7CBE	**Type :** data **MD5 :** a3171cbdc49ddab474d5ac2e67220abb **SHA-1 :** 557aa9da185b48788329acf58a30e76b0cab47c2 **SHA-256 :** 15d6dd96c0c42a0069275974bfcf168525abbdaa **SHA-512 :** 87fd552c4a71712c18378d3df133aaf4a080ed9e **Size :** 1.66 Kilobytes.
C:\Users\User\AppData\Local\Temp\SwuEFE3.Tmp	**Type :** bzip2 compressed data, block size = 900k **MD5 :** 15c26db394c8ba844517b13236749487 **SHA-1 :** 1e27c6f65463c6ab2f26489aa4321003ef02f4b9 **SHA-256 :** 483571a2f005509f1ea68cd2f8d62e265a2ca6bc1 **SHA-512 :** 33aff54cf06f4a80aeca3a0fccc2c1e36bb23d5418 **Size :** 8811.737 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** fa9cbcb2f424dd9465fd31dcdf9f6561 **SHA-1 :** dc3bfe474e4fab8b51954b01e49f92175c89a376 **SHA-256 :** 15e40ad3b5c322d4c0735a1723403f8d29a6dda3 **SHA-512 :** 8a41b3095fde1fe31a63264d91a5e65f2798ae53 **Size :** 5.672 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\9A19ADAD9D098E039450ABBEDD5616EB_04EB95CBF9CF5CBD7E29D6EC69DB8985	**Type :** data **MD5 :** 023fdd2a3a724ba98c143c938844dda1 **SHA-1 :** 066e01a8be031469c733a37f5b2b90d011026427 **SHA-256 :** 7e305d70aeb51debe3a0fbde2c4fea2fc4e255a7 **SHA-512 :** 29826dafca2e6c3d030ae152679a04e61666256c **Size :** 0.394 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db	**Type :** SQLite 3.x database **MD5 :** 54fe29a4ee289ba5a543cc671f9e1b9d **SHA-1 :** d571805f76ea744b0ce64d605de13511b514bcda **SHA-256 :** a727c7ad19e5f949cfb3701bbc0faf204d90b3810 **SHA-512 :** d2ef2f2c7b618a336dc171dc71eb22d5987f29d1 **Size :** 9.216 Kilobytes.
C:\Windows\Tasks\DriverUpdate Scan.Job	**Type :** VAX-order 68k Blit mpx/mux executable **MD5 :** 9850801d4a91f60e5d426c5b27251e38 **SHA-1 :** 270d645a3cb355a3628d208187af18276fb17e4c **SHA-256 :** f3570353a1237d61b05b9f2e14c640b684ae9585 **SHA-512 :** 7ffc996dc82ffa2c516697e01ea2175c1bb648d4a **Size :** 0.446 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Logs\2018-08-19 10-14-56 0.Log	**Type :** ASCII text, with very long lines, with CRLF line terminators **MD5 :** 9a3479819126fc4e8fc1ff51962693d4 **SHA-1 :** 42a518eee9bffd8490a58689a7d8c8fd3a51f166 **SHA-256 :** 44683697ddcbcf8eac9bfc758d3059317d3c8c8c9 **SHA-512 :** 540c2fc9932845836443ca9561cb1a3b6095fb5fb **Size :** 2.514 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7D266D9E1E69FA1EEFB9699B009B34C8_0A9BFDD75B598C2110CBF610C078E6E6	**Type :** data **MD5 :** 5e9e98ceccd4919b1dfa09315cb94153 **SHA-1 :** 6dc74bfe0811762532fc3c8c076138d8e112df40 **SHA-256 :** 71a7891c936aafeedff9431691e858f73c821b6a5 **SHA-512 :** 765cb4ecc7e2cccae433fdf8ceb816ea96ee6eeb6 **Size :** 0.404 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 50195a7d66ef51d81dba6a47e0f9508e **SHA-1 :** da185e19938a8723914a281a773704e54aa04376 **SHA-256 :** 9b21260f896996c39026945455890574a1bb854 **SHA-512 :** db60e799663c4c6825a4f0beec9f83663e0692bc **Size :** 1.544 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 33dcc2eae93098b72dfad23b6041f577 **SHA-1 :** 5a3d21947a09cc41f1a559f12122a941410906cf **SHA-256 :** b3b5dc788b6ee6c96021753279ea2f18f82433bb **SHA-512 :** 8e003789bc3d8482e5afc7fb45ab534ebf90968d **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 33cc12344c91092079a98ecfd93d2b53 **SHA-1 :** f6d80180ce119e4c34886b67d81e888a1ac416c2 **SHA-256 :** a60628a1b06147f7b522b70d03a4ae541502028 **SHA-512 :** 6833b341f14923603e66f9496bff282014f711475 **Size :** 5.672 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\9A19ADAD9D098E039450ABBEDD5616EB_90968CAB679DC8A66D51322A089E7CBE	**Type :** data **MD5 :** 755ed1180e07377aa19b243be495480c **SHA-1 :** 084e5222e0d3cb420674512b2232aaf332b98410 **SHA-256 :** 55bb2bd8338544451892ad6949e9a0c7567dfc6 **SHA-512 :** df9355e25e91f4a5743be2d014e0c72cf9b4a809 **Size :** 0.398 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 2c6238f63996c9e1fad367d1b691400e **SHA-1 :** ac07ec70ae5a8728b926880d3376791f0091dc94 **SHA-256 :** edc4c137524a99f9d3ba74a1002925a6bd8c84c0 **SHA-512 :** 75c6c684cc13fc8a5e441452c8ffb2a8418be8734 **Size :** 2.576 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 3db27759b898158bc247daae38539685 **SHA-1 :** afe86ed37a36fcc4f3fe5d0cb9b89cd3aca74ca3 **SHA-256 :** 353ea8a1f383369db0985cc413654fefcd4f68c8e **SHA-512 :** 12e9b14c0f5d13ff37a3d93aa72c3d765ecbd5afd **Size :** 2.576 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** b7e791ada3ca5c47d81f75ab674452e5 **SHA-1 :** 9c7033231d44fb21fc5c698792f9f51e40ab7d2b **SHA-256 :** d38c48bb8a59fd95a8f7eaf660bd5a7f4640f1e4c **SHA-512 :** 80d22a39ba34db7003ca61c36518b87619b5b93 **Size :** 5.672 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** f6f9cd66950dbe06042d78b0a1ee46b5 **SHA-1 :** 3652b7e216396cda4bedabd73d4ce9d2cc7412b8 **SHA-256 :** a205dae80e3b594a8b76ec94b1d7b5031cddb26 **SHA-512 :** 1616285fc01b21aa4f42a3e298f30fd4d2b896bcc **Size :** 5.672 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\9A19ADAD9D098E039450ABBEDD5616EB_04EB95CBF9CF5CBD7E29D6EC69DB8985	**Type :** data **MD5 :** 27af62756bd7d94203edae66bf710e36 **SHA-1 :** ca38ab2f41a424f96a3b51eafff7da20c3989807 **SHA-256 :** a4bd91dd52321b342da3f4755ce3918a2bae659 **SHA-512 :** fc95c538af75036567da4e00204f1f96b3f247dfd **Size :** 1.66 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7D266D9E1E69FA1EEFB9699B009B34C8_0A9BFDD75B598C2110CBF610C078E6E6	**Type :** data **MD5 :** b1590e957d68224d5092d972e1b73f33 **SHA-1 :** 587723366b5fdbd9300c90e5f59807bc71325566 **SHA-256 :** 5feadb157965eb116b819640195be4f8d3b0c722 **SHA-512 :** 18819c3f672261fbfe83aa46ee6825001e921b67 **Size :** 1.754 Kilobytes.
C:\Users\User\AppData\Local\Temp\MSIeed3b.LOG	**Type :** Little-endian UTF-16 Unicode text, with very long lines, with CRLF line terminators **MD5 :** 830b3c16e9d22b8b0470ab0997a2e6b5 **SHA-1 :** 2d3dc8ec8464563c954eb2981ae200b01bcfc6f9 **SHA-256 :** b4bf6fe6bb9283aa71c40c0f1e77ed8856508fd7c **SHA-512 :** 9c485e02d81e554abd2a0a54c94ad93c1eb7f2c4 **Size :** 382.798 Kilobytes.
C:\Users\User\AppData\Local\Temp\MSIeece6.LOG	**Type :** Little-endian UTF-16 Unicode text, with very long lines, with CRLF line terminators **MD5 :** 19c188bccf3b0d3796e19771407f9fc1 **SHA-1 :** 4239c672fb0cc5009f52283c28f106c2290f4422 **SHA-256 :** a33f7308a3415a0d3f0a439e6db6cb40d065c426 **SHA-512 :** 068826f419142aae104dc30978bb4c95a1fe941b **Size :** 245.2 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 1f4a4d457d6663abc00b3c2b4c6979b9 **SHA-1 :** 2712268fab6713ebeebff76214142eabb32dde1b **SHA-256 :** c2cf77e1ad282ed9f67c9b726ddf2841d7547f77f **SHA-512 :** d7c4afc1c8070297ae420e6fa9b2eee6f88dc702f **Size :** 2.576 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 36711aa05ea4650ba448c639ac342685 **SHA-1 :** d54818afa4f076a4a78409508e7473ad62f4dfd2 **SHA-256 :** a91a1213b7d88a4544bc6b7ef605f554d6b8f6b3 **SHA-512 :** 8ebbe38b6347540a33cf4f111e335643ff532f424 **Size :** 2.576 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 27051dba5c9d3e846ccc12b878a0e5ff **SHA-1 :** 909113ab56b75760e1cdaffb0dacbfa77a9eb390 **SHA-256 :** 193939eac0f94051d71d55223f495d53d28c6fc03 **SHA-512 :** b37298eb30d43503fbea2b42ea44e3b99c4dbc6 **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 58c0653d677cf7fa4e3b3cee4ee0d2ed **SHA-1 :** 027654804e8ada399328c7042314d0d39bcd0666 **SHA-256 :** bfd6d773242f1cd4127d87b3c43868c0b43ce4c2 **SHA-512 :** 87a6db837566a0071a265ad40039a5c5318d956 **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 06de636ca0251cc3f77aa7f9b84e5907 **SHA-1 :** 0f3e32e24c6e3fd73f27c25286ba6751d09c3841 **SHA-256 :** 017e6131807367827a9d8ff1c6118741b02d0a2b **SHA-512 :** 8cb8a22ac2b5c01257149a8e54e3dce8ca9382ab **Size :** 5.672 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 8b2fe5c4586db1be33a231220bfefe5e **SHA-1 :** 171c13bc95516573976165f165b28525593a1e66 **SHA-256 :** 4994eb37719c9205e85d874f3ed203a26d07192 **SHA-512 :** dda0a00cf98242c81f5863552f4c18b37cc0148ff7 **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\Temp\SIOUT9346578\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 :** 5f4a74ec370321ca051037bb363b1440 **SHA-1 :** df1b725181d75f5078136eaf04d2a8e2b16c6952 **SHA-256 :** 22248a2ade7842e229afbdc6e1d3929b45bf64b1 **SHA-512 :** 6baa79f8263a2290dffc5ea05db7c0aee1569785 **Size :** 1.544 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 59c49aa45ab489baa7a883440a090104 **SHA-1 :** 62bdaab29efb26cce59a3b6d5d787eb62d771404 **SHA-256 :** df3dfa177ceed008b35fc269e55936ec12d0b9da **SHA-512 :** 752850b58f7e3b02156436f9c16da64d3cc7f799 **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\Temp\ScpAB0.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\Settings.Db-Journal	**Type :** data **MD5 :** 2115bce422b189b08f672ec314a18d6f **SHA-1 :** 0613e2522eddacc3fe62598ff7c95dbb74a08a41 **SHA-256 :** 04bf6048b4b1475edb0c3d9ceab2ad08ebc6f87c **SHA-512 :** 606062c8ec93134c7e561a1b60bf23d1b684f6d5 **Size :** 1.544 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 2d26ef5dff21880163a31a3a124de67c **SHA-1 :** 50bd77b96803863ac8cb9b7018c08886d706fd0b **SHA-256 :** a5fac241578b2e14175cffa31aeb23b488271fb96 **SHA-512 :** 8214b9aeebf66b7aa94793097967cf256b4dfb98 **Size :** 2.576 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** de9e1ee1141b464549957dd6c2152b31 **SHA-1 :** 5be08df5f12e41fc355dcd3d4246988354e2170b **SHA-256 :** 782b824e314142f0e8c5b13cd3de2e41233a033e **SHA-512 :** dc067b099a3333ec63f8d2ad08812a5af830f13d7 **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** deb59a75b47692f2f9dfc6c995b56802 **SHA-1 :** 1ae693b179801724b3ded34fe56ef4f44279328a **SHA-256 :** 71706133d3c930f7a8b1032c565f666211d39f5b **SHA-512 :** ff6e01ffbb5fbe3d7560dfc47136efe4cc3e12b73b **Size :** 2.576 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 :** e6dad1d7888193acb08983685188ed39 **SHA-1 :** 48e5d073e705f221c68f44d424e35c4e039c6a52 **SHA-256 :** 208861c51970fbe452d4f3a91653f841a78aa50e **SHA-512 :** fe62e1dcf279cf339b98e481bff1827d6b36f15e0c **Size :** 2.576 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 562e5b1f0dc2d579eabdb034c56f0720 **SHA-1 :** fc580582fd5c1635cf3bb8efef5123e92377bff8 **SHA-256 :** 31cfe7dd35fa79e8fd331055da5a2af9aff995bf38 **SHA-512 :** d5269e4ce4f8175d64da24b231680ee4897ae298 **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** f1e434cbbfdb3f0bafe2f8e64e6698eb **SHA-1 :** 78634489819b922f2cec133554ccda4d137b1798 **SHA-256 :** 7fa3cb0f18f756040217d4de5227bcc6adba53fe5 **SHA-512 :** 4cd19b6aae6757232e3b46d435b65b52b74406c **Size :** 0.342 Kilobytes.
C:\Windows\Sysnative\Tasks\DriverUpdate Scan	**Type :** XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators **MD5 :** dad43414d629c23b1ec7fd09a10d1cdb **SHA-1 :** ce4b8004ddfe3fa6b0ffb7e90953e58abeb74f88 **SHA-256 :** ab67d95f9625d3953e8c2f8795e150ec57f6420f3 **SHA-512 :** 2124feee26cae3007bdd6c89cb30bafe26abc084 **Size :** 3.172 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** e19730bc9b809fcba75b2b2bc8c53b69 **SHA-1 :** a619728474893ee55a800d29341284eb4f3a9a4e **SHA-256 :** 80a1a8a87d7fe0c78d2bc6574923533a86f6f26f7 **SHA-512 :** c3f112e76ea9cf4740a2ad5b76e9f9bfa3b9b9255 **Size :** 5.672 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 496db6fdd3d8aa68a499c7fdd8bd5d9b **SHA-1 :** c5600e2b02aaa2e8e005b74b800b7a2634005f1a **SHA-256 :** 824d3fa30bc73bae85318d0d5f6e309d24840728 **SHA-512 :** 19f6193d2f415e769e1bcd69e95edbe6cbfbe28e **Size :** 6.704 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	None
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	3776b000b8b93bee018a98b1338bac5b9eb18383
MD5:	
First Seen Date:	2018-08-18 14:40:19.679062 (9 months ago)
Number Of Clients Seen:	2
Last Analysis Date:	2018-08-18 14:40:19.679062 (9 months ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[{u'Path': u'E:\\BuildAgent\\work\\652325c68c8b38d0\\bin\\Release\\LittleInstaller.pdb\x00', u'GUID': u'{5337e2ad-9141-4845-bcde-61c5f9474a11}', u'timestamp': u'2017-10-20 21:42:05'}]
Number Of Sections	5
Trid	[[36.1, u'InstallShield setup'], [26.2, u'Win32 Executable MS Visual C++ (generic)'], [23.2, u'Win64 Executable (generic)'], [5.5, u'Win32 Dynamic Link Library (generic)'], [3.7, u'Win32 Executable (generic)']]
Compilation Time Stamp	0x59EA6DAD [Fri Oct 20 21:42:05 2017 UTC]
LegalCopyright	Copyright 2011-2016 Slimware Utilities Holdings, Inc.
InternalName	LittleInstaller
FileVersion	2.9.4
CompanyName	Slimware Utilities Holdings, Inc.
ProductName	DriverUpdate
ProductVersion	2.9.4
FileDescription	DriverUpdate Setup Wizard
OriginalFilename	DriverUpdate-setup.exe
Translation	0x0409 0x04b0
Entry Point	0x439175 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	1015448
Ssdeep	
Sha256	e0f24fe91c7e1f16486006361f3dc500e741d9ce43ccf576ab27a4fd178321ed
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	9ca88b0a442d45060e56bb1d965ff0fa

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x5be88	0x5c000	6.6452169074	4b02fa5707fbd46ab060dfda6072caf7
.rdata	0x5d000	0x18ed0	0x19000	4.72133560729	4442b1d0d2b3d7f258d30180401f5af1
.data	0x76000	0x81fc	0x5000	4.10584349386	7b8018dd53c60812d1dc56b299398836
.rsrc	0x7f000	0x6ab6e	0x6b000	5.7944070136	498c0d0146574b5eb7e80f9862839bfb
.reloc	0xea000	0xcdde	0xd000	4.23612853678	55d244ad9eacae24b95dd8ef88d81bc6

PE Imports

- PSAPI.DLL
  - GetProcessImageFileNameW
  - EnumProcesses
- KERNEL32.dll
  - GlobalFlags
  - TlsGetValue
  - GlobalReAlloc
  - GlobalHandle
  - TlsAlloc
  - TlsSetValue
  - LocalReAlloc
  - TlsFree
  - SetErrorMode
  - HeapFree
  - HeapAlloc
  - GetProcessHeap
  - GetStartupInfoW
  - ExitProcess
  - TerminateProcess
  - UnhandledExceptionFilter
  - SetUnhandledExceptionFilter
  - IsDebuggerPresent
  - HeapReAlloc
  - RtlUnwind
  - SetStdHandle
  - GetFileType
  - ExitThread
  - CreateThread
  - HeapSize
  - VirtualAlloc
  - WritePrivateProfileStringW
  - GetModuleFileNameA
  - FreeEnvironmentStringsA
  - GetEnvironmentStrings
  - FreeEnvironmentStringsW
  - GetEnvironmentStringsW
  - GetCommandLineA
  - GetCommandLineW
  - SetHandleCount
  - GetStartupInfoA
  - HeapDestroy
  - HeapCreate
  - VirtualFree
  - QueryPerformanceCounter
  - GetSystemTimeAsFileTime
  - GetCPInfo
  - GetACP
  - GetOEMCP
  - IsValidCodePage
  - GetTimeFormatA
  - GetDateFormatA
  - GetTimeZoneInformation
  - LCMapStringA
  - LCMapStringW
  - GetConsoleCP
  - GetConsoleMode
  - GetStringTypeA
  - GetStringTypeW
  - GetUserDefaultLCID

- GetLocaleInfoA
- EnumSystemLocalesA
- IsValidLocale
- WriteConsoleA
- GetConsoleOutputCP
- WriteConsoleW
- CreateFileA
- SetEnvironmentVariableA
- ReleaseMutex
- CreateMutexW
- GetCurrentThread
- ConvertDefaultLocale
- GetVersion
- EnumResourceLanguagesW
- GetLocaleInfoW
- LoadLibraryExW
- CompareStringA
- CreateEventW
- SuspendThread
- SetEvent
- ResumeThread
- SetThreadPriority
- lstrcmpA
- GetFullPathNameW
- GetVolumeInformationW
- DuplicateHandle
- SetEndOfFile
- UnlockFile
- LockFile
- WriteFile
- GetThreadLocale
- GetFileTime
- GetFileAttributesW
- FindFirstFileW
- FindClose
- GetModuleHandleA
- GlobalAddAtomW
- GlobalFindAtomW
- GlobalDeleteAtom
- CompareStringW
- lstrcmpW
- GetVersionExA
- GlobalLock
- GlobalUnlock
- FreeResource
- GlobalFree
- GlobalAlloc
- lstrlenA
- GetFileSize
- CreateFileMappingW
- MapViewOfFileEx
- UnmapViewOfFile
- GetFileSizeEx
- FindResourceExW
- LoadLibraryA
- InterlockedExchange
- FreeLibrary
- LocalAlloc
- GetUserDefaultUILanguage
- OpenProcess
- WideCharToMultiByte
- ExpandEnvironmentStringsW
- InterlockedDecrement
- InterlockedIncrement
- LeaveCriticalSection
- DeleteCriticalSection
- InitializeCriticalSection
- MoveFileExW
- EnterCriticalSection
- ReadFile
- SetFilePointer
- FlushFileBuffers
- GetCurrentProcess
- GetCurrentProcessId
- GetCurrentThreadId

    - CreateFileW
    - GetSystemDirectoryW
    - GetTempFileNameW
    - SetDllDirectoryW
    - GetTempPathW
    - OutputDebugStringW
    - RaiseException
    - VerSetConditionMask
    - VerifyVersionInfoW
    - GetExitCodeProcess
    - DeleteFileW
    - MoveFileW
    - CopyFileW
    - CreateDirectoryW
    - MultiByteToWideChar
    - GetVersionExW
    - WaitForSingleObject
    - Sleep
    - OpenEventW
    - MulDiv
    - CloseHandle
    - CreateProcessW
    - GetTickCount
    - lstrlenW
    - FileTimeToLocalFileTime
    - FileTimeToSystemTime
    - GetUserDefaultLangID
    - GetModuleFileNameW
    - GetProcAddress
    - LoadLibraryW
    - SetLastError
    - GetModuleHandleW
    - GetLastError
    - LoadResource
    - LockResource
    - SizeofResource
    - LocalFree
    - FormatMessageW
    - FindResourceW
    - GetStdHandle
- USER32.dll
    - DestroyMenu
    - GetMessageW
    - TranslateMessage
    - ValidateRect
    - CharUpperW
    - EndPaint
    - BeginPaint
    - SetMenuItemBitmaps
    - GetMenuCheckMarkDimensions
    - LoadBitmapW
    - ModifyMenuW
    - GetMenuState
    - CheckMenuItem
    - RegisterWindowMessageW
    - SendDlgItemMessageA
    - WinHelpW
    - GetCapture
    - SetWindowsHookExW
    - CallNextHookEx
    - GetClassLongW
    - SetPropW
    - GetPropW
    - RemovePropW
    - GetLastActivePopup
    - DispatchMessageW
    - GetTopWindow
    - UnhookWindowsHookEx
    - GetMessageTime
    - GetMessagePos
    - PeekMessageW
    - MapWindowPoints
    - GetKeyState
    - UpdateWindow
    - GetMenu

- GetSubMenu
- GetMenuItemID
- GetMenuItemCount
- CreateWindowExW
- GetClassInfoExW
- GetClassInfoW
- RegisterClassW
- DefWindowProcW
- CallWindowProcW
- SystemParametersInfoA
- IsIconic
- GetWindowPlacement
- GetWindowTextW
- GetFocus
- SetFocus
- MoveWindow
- IsDialogMessageW
- IsDlgButtonChecked
- SetDlgItemTextW
- SendDlgItemMessageW
- CheckDlgButton
- GetDesktopWindow
- GetActiveWindow
- SetActiveWindow
- GetSystemMetrics
- CreateDialogIndirectParamW
- DestroyWindow
- GetDlgItem
- IsWindowEnabled
- GetNextDlgTabItem
- EndDialog
- EnumThreadWindows
- WaitForInputIdle
- ShowWindow
- ClientToScreen
- ScreenToClient
- ReleaseCapture
- SetCapture
- InvalidateRect
- ReleaseDC
- GetDC
- SetRectEmpty
- PtInRect
- TrackMouseEvent
- LoadCursorW
- SetCursor
- SetWindowTextW
- EnumChildWindows
- GetDlgCtrlID
- GetSysColorBrush
- GetClientRect
- FillRect
- IsWindowVisible
- GetWindowThreadProcessId
- MessageBoxW
- EnumWindows
- SetForegroundWindow
- PostQuitMessage
- RegisterClipboardFormatW
- SetWindowPos
- GetClassNameW
- UnregisterClassW
- DestroyAcceleratorTable
- GetParent
- TranslateAcceleratorW
- OffsetRect
- EnableMenuItem
- AdjustWindowRectEx
- CreateAcceleratorTableW
- SetRect
- MessageBeep
- MapDialogRect
- GetCursorPos
- IsWindow
- GrayStringW

    - DrawTextExW
    - DrawTextW
    - TabbedTextOutW
    - GetWindowLongW
    - SetWindowLongW
    - PostMessageW
    - GetForegroundWindow
    - AppendMenuW
    - GetSystemMenu
    - LoadIconW
    - PostThreadMessageW
    - FindWindowW
    - CloseWindow
    - GetWindow
    - SetTimer
    - KillTimer
    - IsRectEmpty
    - CopyRect
    - GetSysColor
    - RedrawWindow
    - GetWindowRect
    - SendMessageW
    - EnableWindow
    - GetWindowTextLengthW
    - UnregisterClassA
- GDI32.dll
    - DeleteDC
    - GetStockObject
    - DPtoLP
    - MoveToEx
    - LineTo
    - ScaleWindowExtEx
    - SetWindowExtEx
    - ScaleViewportExtEx
    - SetViewportExtEx
    - OffsetViewportOrgEx
    - SetViewportOrgEx
    - SelectObject
    - GetTextExtentPoint32W
    - CreateDIBSection
    - DeleteObject
    - SetMapMode
    - SetBkMode
    - RestoreDC
    - SaveDC
    - CreateBitmap
    - SetBkColor
    - SetTextColor
    - GetClipBox
    - GetTextExtentExPointW
    - SelectClipRgn
    - CreateCompatibleBitmap
    - BitBlt
    - SetBrushOrgEx
    - CreateCompatibleDC
    - CreatePatternBrush
    - GetDeviceCaps
    - CreatePen
    - CreateSolidBrush
    - GetTextMetricsW
    - Rectangle
    - Escape
    - ExtTextOutW
    - TextOutW
    - RectVisible
    - PtVisible
    - CreateFontIndirectW
    - GetObjectW
- COMDLG32.dll
    - GetFileTitleW
- WINSPOOL.DRV
    - OpenPrinterW
    - DocumentPropertiesW
    - ClosePrinter
- ADVAPI32.dll

    - RegEnumKeyExW
    - RegQueryValueW
    - RegEnumKeyW
    - RegOpenKeyW
    - RegDeleteValueW
    - RegDeleteKeyW
    - RegEnumValueW
    - RegSetValueExW
    - RegQueryInfoKeyW
    - RegCreateKeyExW
    - RegQueryValueExW
    - RegOpenKeyExW
    - RegCloseKey
- SHELL32.dll
    - ShellExecuteW
    - SHGetFolderPathW
    - CommandLineToArgvW
    - Shell_NotifyIconW
- COMCTL32.dll
    - InitCommonControlsEx
- SHLWAPI.dll
    - SHCreateStreamOnFileEx
    - SHRegGetUSValueW
    - PathAppendW
    - PathFileExistsW
    - AssocQueryStringW
    - StrStrIW
    - PathStripToRootW
    - PathIsUNCW
    - PathFindFileNameW
    - PathFindExtensionW
    - UrlEscapeW
- ole32.dll
    - CoFreeUnusedLibraries
    - CoInitialize
    - CoTaskMemFree
    - StringFromCLSID
    - CoCreateInstance
    - StringFromGUID2
    - CoCreateGuid
    - CoUninitialize
    - CoInitializeEx
    - OleInitialize
    - OleUninitialize
    - CoRevokeClassObject
    - OleIsCurrentClipboard
    - OleFlushClipboard
    - CoRegisterMessageFilter
- OLEAUT32.dll
    - SysAllocStringLen
    - VarBstrCmp
    - LoadTypeLib
    - LoadRegTypeLib
    - VariantChangeType
    - SysStringLen
    - VariantClear
    - SysAllocString
    - VariantInit
    - SysFreeString
- WS2_32.dll
    - WSAStartup

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 524960, u'sha256': u'fbeb3be87e80cb8e1d2af3d8140796c1bb80c6c7056f60897088ff9e355c3867', u'type': u'data', u'size': 308}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 525268, u'sha256': u'f64ccc0582bc7c66af8b40049e485e8e241335261ec95ace909293ba50b2e4a3', u'type': u'data', u'size': 180}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 525448, u'sha256': u'e7c0005285d1ab59732d5f99f77a9bdd6342b01cf44437ebd7a07611a227e272', u'type': u'data', u'size': 184}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 525632, u'sha256': u'abdf36bde89a26349f5741c17c235dacea88d441d8662ba16a598dc50c3c4864', u'type': u'data', u'size': 324}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 525956, u'sha256': u'ca8fc96218d0a7e691dd7b95da05a27246439822d09b829af240523b28fd5bb3', u'type': u'data', u'size': 744}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 526700, 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': 526996, u'sha256': u'3bbacbad1458254c59ad7d0fd9bea998d46b70b8f8dcfc56aad561a293ffdae3', u'type': u'data', u'size': 2216}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 529212, 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': 530596, u'sha256': u'6e4c3f9044eaf9d157ec8e50bc8a5cd9069b6078058094a4b4a4ab8e6e1ffac1', u'type': u'data', u'size': 68}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 530664, u'sha256': u'300f275bbb1008b2a4367954d64a08db87c680c7bdd0c03615c3a37cfc61a0a9', u'type': u'data', u'size': 366}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 531032, u'sha256': u'4f74a949fe2c9358a546f41a9c598fbe326b432ff17dfbacf2842ac6e7d1787a', u'type': u'data', u'size': 332}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 531364, u'sha256': u'b89eec935455ed0f590248a8446072a56ccc12ab66583b2e54719ec5cf4e2bc1', u'type': u'data', u'size': 362}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 531728, u'sha256': u'62baabd903384fbf221e1149d05900356bd2286c2567e2ce231ee7d168692afe', u'type': u'data', u'size': 526}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 532256, u'sha256': u'e432c7e74e96b328e317b2d14908c0030eabaeecd3edb4c9df6fc0c2b160ac45', u'type': u'data', u'size': 286}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 532544, u'sha256': u'3b442c077a3c0edd83101d47295701259db768024978619fce3b978e4ccdebdc', u'type': u'data', u'size': 462}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 533008, u'sha256': u'd740b552c6f5879f3193780de45a419aea68ed0e24f1ae2857115f661adc3052', u'type': u'data', u'size': 376}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 533384, u'sha256': u'0da23009e825ebab541af8804f12bf6d64497bd2efb4635a6b8b97ebbb9c84b0', u'type': u'data', u'size': 518}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 533904, u'sha256': u'4cf716efaf68e0cb2ec45ec55d291050b5712b05653cae68edbb999f803d2a98', u'type': u'data', u'size': 52}

{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 533956, 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': 534176, 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': 534388, 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': 534592, 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': 534764, 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': 534860, u'sha256': u'4803a1975883eb60af94b51e9532e228976461273c7371f3cd133aa4e785819b', u'type': u'data', u'size': 98}

{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 534960, u'sha256': u'f39b611bd7fd6cf6911947fec504ddde1603149502b794c3f8bb28aa4c088c5f', u'type': u'data', u'size': 120}

{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 535080, u'sha256': u'ba847dbbcbb4d05fcf8c5c6ca8dbe2e8f1bef3c8ba5bd1862fe1644b2dd73156', u'type': u'data', u'size': 128}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 535208, u'sha256': u'81f3a5cb443e8ad28345f14d4f2ff55aae85e56f3058489e75172ca1164e131d', u'type': u'data', u'size': 82}

{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 535292, u'sha256': u'258d51f0e31fb7e76662e90b0b6f7276eea18dd7be38bb2f37a883617db56c7a', u'type': u'data', u'size': 68}

{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 535360, u'sha256': u'08c792e3e0c8c773892a51fc5f1acfabd6bf5556e5e05f33c728e8bec4577610', u'type': u'data', u'size': 258}

{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 535620, u'sha256': u'da54b5e20f2459b9a25d8b22005d66a8a24dcfdbf5fca99893d5d08515d25586', u'type': u'data', u'size': 314}

{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 535936, u'sha256': u'fc0ac66e26e5951aa62080e9f15920e54c6aded25923c43f401b69f232a940a6', u'type': u'data', u'size': 340}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 536276, u'sha256': u'897f48ffd80577b462e07038911df69b1607a270b0d83a024c0b7a78361d6aee', u'type': u'data', u'size': 228}

{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 536504, u'sha256': u'f5f2d753d1a3986f3ce3a955d2b2a1d5af05c5dc69e3a6567f8b75541f0f0db0', u'type': u'data', u'size': 174}

{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 536680, u'sha256': u'40c1b95e6f501edd0ebff2a2736f38e94f9930b76bfe0a28fed3dd62b1ab47c8', u'type': u'data', u'size': 594}

{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 537276, u'sha256': u'1056298d4517e7cedfe80bac785d9a4e0fc7b4df0bd1847bf1727a3c259aa2b8', u'type': u'data', u'size': 480}

{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 537756, u'sha256': u'06025e6f9616ddd627cdca09aac5653e9c890e03c8408f8d4db58a8883c9f19a', u'type': u'data', u'size': 516}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 538272, u'sha256': u'1e5598008e22ef78ff73e17947e5980ffbfbbe8f7d5dd3cf2d8e34e28f175eeb', u'type': u'data', u'size': 380}

{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 538652, u'sha256':

u'309f434d357a58c314d921e23f3411e90628698a9375dfe689281617ff688267', u'type': u'data', u'size': 228}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 538880, u'sha256': u'855d77f3f6ad12a99586b3f021cb2921abaa0504d20855b8c43b314075b26705', u'type': u'data', u'size': 922}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 539804, u'sha256': u'd8f42d3f98d8914f22f4c4d5191487b72903dd1e0905e3bf0986e3b794c29762', u'type': u'data', u'size': 912}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 540716, u'sha256': u'4397ec8a8f18cf20dd80aa59705298089efa88a444cde61ddaaac9fee0e5ea4a', u'type': u'data', u'size': 938}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 541656, u'sha256': u'1bd8125d5560f1f89cbbf579f9e6e217a0b9499484a3a7f41e6f5c464301ef60', u'type': u'data', u'size': 718}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 542376, u'sha256': u'c5029792d1423ed28055deeda7745563f4f78dcdaa0dbd6b610af7631a433acc', u'type': u'data', u'size': 554}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 542932, u'sha256': u'84050bef84e46fe781f9c5ac7cb30985aef90b23beb97bc425a6fae49cf3cb6a', u'type': u'data', u'size': 290}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 543224, u'sha256': u'ad279e11c370d3e636cf8167bef1a9ea82282bccd80431a100c86d314297d25c', u'type': u'data', u'size': 284}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 543508, u'sha256': u'8d88449cff57219d23f311779473047b16e7efe62f8077e5f053b40931358c0b', u'type': u'data', u'size': 286}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 543796, u'sha256': u'90473bb9384f3f39541eabad15e612fe7c8cd555cbca23fbb06d05ac90aa29a3', u'type': u'data', u'size': 296}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 544092, u'sha256': u'814bebef4ed9fd87c501e2d52feef223193d9a9859a9d0e9a9beca3b69ef7012', u'type': u'data', u'size': 212}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 544304, u'sha256': u'0947cde4cd80ac726e4d7d5d5d966bf16ea1dba641df74265d529724d369d33f', u'type': u'data', u'size': 378}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 544684, u'sha256': u'b69faeb1cc99f8532806c8bf35d553b6ca8293fe32bbd7bd1e2cdfa3d19096ed', u'type': u'data', u'size': 360}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 545044, u'sha256': u'a246ce2c4837b1fbe3d54ed158ffd8fe727105418327bd1f8029263365005412', u'type': u'data', u'size': 344}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 545388, u'sha256': u'fb8e67ea0b8787e4ed24ca15731be79548d684699746bc53a8d3e228f4e71de1', u'type': u'data', u'size': 280}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 545668, u'sha256': u'a7e3c29df3af8134eb884624ec3636b227f5b922d703c3129221986366a749e1', u'type': u'data', u'size': 172}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 545840, u'sha256': u'2ad80490bfbd67e316b34a78c166dfbc8ddbbbac2ac5d3232692fc77dfa32de1', u'type': u'data', u'size': 438}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 546280, u'sha256': u'2cfe0e6e9d5cd1695f2f1028e9936286288f0408d246457ce99509303c1f908f', u'type': u'data', u'size': 426}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 546708, u'sha256': u'fcadde9f221c77e92a26007a43313154e345e09d952ebf6adfa84d2341cc8fa7', u'type': u'data', u'size': 426}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 547136, u'sha256': u'409664bc384377038c8e17156195a88f6819c0273530d451a3edbc0ebe4b9342', u'type': u'data', u'size': 396}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 547532, u'sha256': u'0d10bf879173f9136af0bd077627063c43b2e5609b7bfba7f158544f4429e2e6', u'type': u'data', u'size': 300}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 547832, u'sha256': u'e88dc92545245cc91e1a61519b7e33747e988e10e89d5ca6c41aa657efeb2f17', u'type': u'data', u'size': 1010}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 548844, u'sha256': u'60add2422a8719abd745ceeb5fbbb37b96e8c9d6df56fac28c25866f7ec90375', u'type': u'data', u'size': 1058}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 549904, u'sha256': u'd4ceb9eecd4216007ae0b18cc2e19af9b1459b5dfa7337368f7b7bfde4cb37d3', u'type': u'data', u'size': 1090}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 550996, u'sha256': u'da41a57fe1c09e66dc3405808cb223209c0ef7d11c4f3c3fb0f389a2a59b17e4', u'type': u'data', u'size': 926}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 551924, u'sha256': u'b6ed99fbb1c6f6474975f631bd3fa2c13880bf44a49da5d31c26ae8b97dc7416', u'type': u'data', u'size': 788}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 552712, u'sha256': u'a0c2f4fc5a466fda1a6c879e38e6a02c2679a166a855dff600d72cbb12353ef9', u'type': u'data', u'size': 1408}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 554120, u'sha256': u'a8efa60ba5b443fd8048fdd281285d54924802500ab1235a2c5b10a99034c920', u'type': u'data', u'size': 1422}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 555544, u'sha256': u'fe96257d65fa702aff1e703afd9dfe859b97d195898406ae4351ac4f27f1c7b4', u'type': u'data', u'size': 1488}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 557032, u'sha256': u'7ba9fe63361f241a3cf8caf3698f1fd903b3e937b325c8c995c3d93b4affbc9d', u'type': u'data', u'size': 2592}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 559624, u'sha256': u'7efde3ffc6dc73b6cde4f8413bf67ccab44474c3aeebc427baec21c78c1145f6', u'type': u'data', u'size': 940}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 560564, u'sha256': u'93f45374d169f3144568a8fc503e933842df0e4c60df1cf16aa8274ed1f29d2a', u'type': u'data', u'size': 336}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 560900, u'sha256': u'b29d7f3a4e66d5cc11d25538fccbdbea47f3bcddd5f5617d1efe097f62343e4c', u'type': u'data', u'size': 286}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 561188, u'sha256': u'4f6e434070d9e68aaccf5c49ca2d8ccc2a0d4669f280f9b307a82896b7226ad6', u'type': u'data', u'size': 326}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 561516, u'sha256': u'be18d8c081be944d61d27a48dcee6b9ec93070999d93ef1298f945919bd06560', u'type': u'data', u'size': 270}

{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 561788, u'sha256': u'1517597eae294617a5ce7b3ae21708f652659c4aefb70b494f7dde7e00236592', u'type': u'data', u'size': 194}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 561984, u'sha256': u'54e8194c123cb9c249a2e2f4a00a9f688fe77107b3729389a60f7f75e6fb9b45', u'type': u'data', u'size': 1852}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 563836, u'sha256': u'245733eceb7bf3399e2a873c74f50df0c9f1433a181cbc788fc29cf1b1606c0b', u'type': u'data', u'size': 1872}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 565708, u'sha256': u'2cf55e32d9d900a15a8d3d49c4d19bdc4367f574222ec627ee95737206fdb879', u'type': u'data', u'size': 1926}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 567636, u'sha256': u'bf19f78b7282e1497e7fe7d9abf281f34590eb70dc649c3dcd1c8c810b0a1864', u'type': u'data', u'size': 1432}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 569068, u'sha256': u'625939ff8f059ca66ae8302b9123a280b9601173843eece5c9b36f07d96cae48', u'type': u'data', u'size': 776}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 569844, u'sha256': u'fdd8bc88b47eca374a61f4cb9d5b3b48fc98f14ba948decb08375a67a32ad12d', u'type': u'data', u'size': 2518}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 572364, u'sha256': u'35c1a773911ea3445af7e1c8d9d59d79e4acb1b0b912e0493ba66f5944f4b35c', u'type': u'data', u'size': 2426}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 574792, u'sha256': u'7f3c35eea518c224e6d30b1dd8e643656b0f8aadb50eadd1c94ee6062e6b72e4', u'type': u'data', u'size': 2594}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 577388, u'sha256': u'367fa128a761866740230a13139b96c30387fea2db04a65fcef1559bf5c06f09', u'type': u'data', u'size': 1928}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 579316, u'sha256': u'8616baa2d2fa31921f8e52af44924189d65e45c07f5e8fae1bb4c45c3e67e887', u'type': u'data', u'size': 1204}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 580520, u'sha256': u'177584c46c7d734f33223e4c585ef9c97ca33a24e49c76b2f20f16964d531920', u'type': u'data', u'size': 56}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 580576, u'sha256': u'291b9c98b2aff4e003dcc57cf5a0a87eff44e0f7803a27282819d0ac6c3a93aa', u'type': u'data', u'size': 62}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 580640, u'sha256': u'66f1747ba4c17f6fca44818ed98445f01645651c120e72f558245e2df6949d35', u'type': u'data', u'size': 402}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 581044, u'sha256': u'0facb5a0cb3ce6df000a594ad8d6428040190be9aaa982716e0587eab374cac9', u'type': u'data', u'size': 906}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 581952, u'sha256': u'c054645d86387fd491743027e6c2284d6a7262f6aced9321cbc1465cef2b6b1f', u'type': u'data', u'size': 794}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 582748, u'sha256': u'c1bc5318a82ea1a1809618040026851947f6aa5171d904a9e60966f4551ca1a3', u'type': u'data', u'size': 732}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 583480, u'sha256': u'1b8660b0c53b94f3e029de58e56d08c8097a080244e9dc65d4155a9b603820d8', u'type': u'data', u'size': 172}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 583652, u'sha256': u'36db380991291cac5c99e42332efda20210f63985544d95e8fa6ef85bf2bdf8e', u'type': u'data', u'size': 1220}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 584872, u'sha256': u'7f51554313c6765ba649783a942064cdfe6f5a70248a6f56840f71969f87ced0', u'type': u'data', u'size': 612}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 585484, u'sha256': u'1f1b61a7f04edc3691a6c9350132b09929d5bfa1c900f6ff500e55c5ebc63212', u'type': u'data', u'size': 66}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_MESSAGETABLE', u'offset': 585552, u'sha256': u'ef493afd7e7a330a21862c1623e75eab30b223bf04d434d0e4fe006a2d7faef6', u'type': u'data', u'size': 1720}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 587272, 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': 587308, 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': 587372, u'sha256': u'c6506d70b4d876e1b3d2de2caf8f841b468314b0058565dd514021a5cf9301a1', u'type': u'data', u'size': 860}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 588232, 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': 589444, u'sha256': u'1a12454cf61b47cb5b00ccd3b5a7e012a81d8225a894f9b73ea60335d6b9d5f1', u'type': u'data', u'size': 93}
{u'lang': u'LANG_NEUTRAL', u'name': u'30', u'offset': 589540, u'sha256': u'cf5260d05db04a6c040dd17131c2114fbafd19b16c2dc5f6803c86135a6f8d0a', u'type': u'data', u'size': 93}
{u'lang': u'LANG_NEUTRAL', u'name': u'30', u'offset': 589636, u'sha256': u'cf5260d05db04a6c040dd17131c2114fbafd19b16c2dc5f6803c86135a6f8d0a', u'type': u'data', u'size': 93}
{u'lang': u'LANG_NEUTRAL', u'name': u'30', u'offset': 589732, u'sha256': u'cf5260d05db04a6c040dd17131c2114fbafd19b16c2dc5f6803c86135a6f8d0a', u'type': u'data', u'size': 93}
{u'lang': u'LANG_NEUTRAL', u'name': u'31', u'offset': 589828, u'sha256': u'8855508aade16ec573d21e6a485dfd0a7624085c1a14b5ecdd6485de0c6839a4', u'type': u'data', u'size': 5}
{u'lang': u'LANG_NEUTRAL', u'name': u'31', u'offset': 589836, 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': 589840, 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': 589844, 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': 589848, 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': 589852, 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': 589856, 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': 637932, 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': 684092, 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': 734416, 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': 782152, 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': 905808, u'sha256': u'cdab229dd06b1469cb504d1c1c96cc51e3eef9f70082eedf282da7edd14d0d14', u'type': u'data', u'size': 1443}
{u'lang': u'LANG_NEUTRAL', u'name': u'34', u'offset': 907252, 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': 923316, 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': 941908, 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': 944932, 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': 956696, u'sha256': u'4fe703b9d23fa79e54cbf1a0048df015d2c3c108fa9add5042d806fac470fc9f', u'type': u'data', u'size': 598}

CERTIFICATE VALIDATION

- Success ✔

[+] Slimware Utilities Holdings, Inc.	
Status	NotTimeValid (no effect on chain status)
Start Date	2015-02-23 02:00:00
End Date	2018-01-07 01:59:59
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)

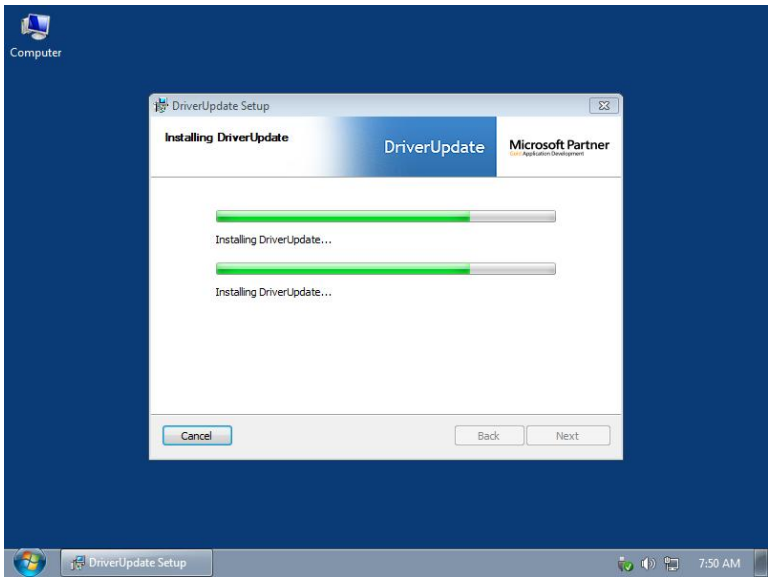
[+] VeriSign Class 3 Code Signing 2010 CA	
Status	NoError ✔
Start Date	2010-02-08 02:00:00
End Date	2020-02-08 01:59:59
Sha256	0f5cd6ebab15fa367e35893fad2bc49cd1a95449f58e7eb978d72bb0b100d764
Serial	5200E5AA2556FC1A86ED96C9D44B33C7
Subject Key Identifier	cf 99 a9 ea 7b 26 f4 4b c9 8e 8f d7 f0 05 26 ef 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)

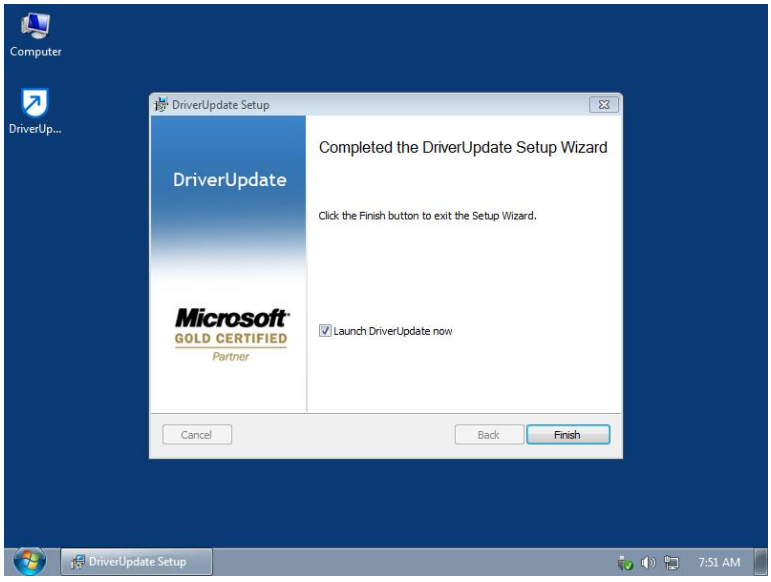
[+] VeriSign Class 3 Public Primary Certification Authority - G5	
Status	NoError ✔
Start Date	2006-11-08 02:00:00
End Date	2036-07-17 02:59:59
Sha256	d0c133d98cabb2199501a761f5b8b9afd30d870477a534b41400a6dc57f5d64d
Serial	18DAD19E267DE8BB4A2158CDCC6B3B4A
Subject Key Identifier	7f d3 65 a7 c2 dd ec bb 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	undefined
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

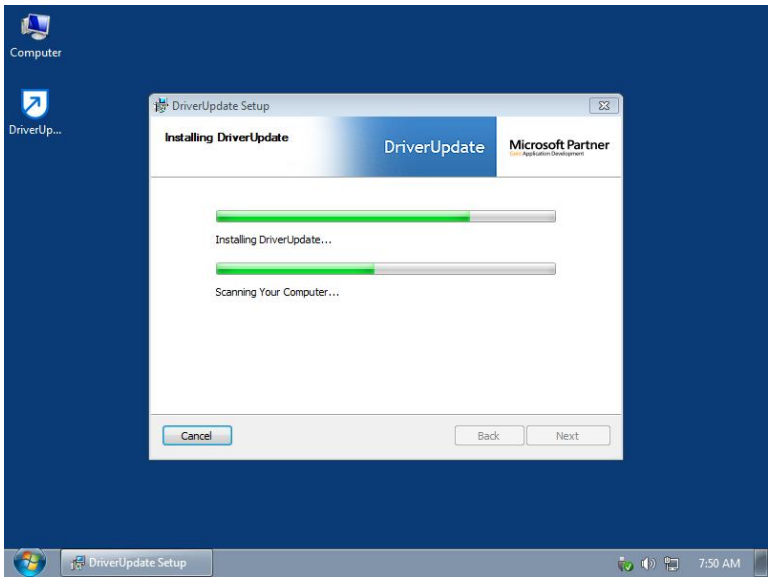
[+] Symantec Time Stamping Services CA - G2	
Status	NoError ✔
Start Date	2012-12-21 02:00:00
End Date	2020-12-31 01:59:59
Sha256	0b44526ab89f4778858bf831045ec218d0d57734caa10208ea3d8c90c1043266
Serial	7E93EBFB7CC64E59EA4B9A77D406FC3B
Subject Key Identifier	5f 9a f5 6e 5c cc cc 74 9a d4 dd 7d ef 3f db ec 4c 80 2e dd
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
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)

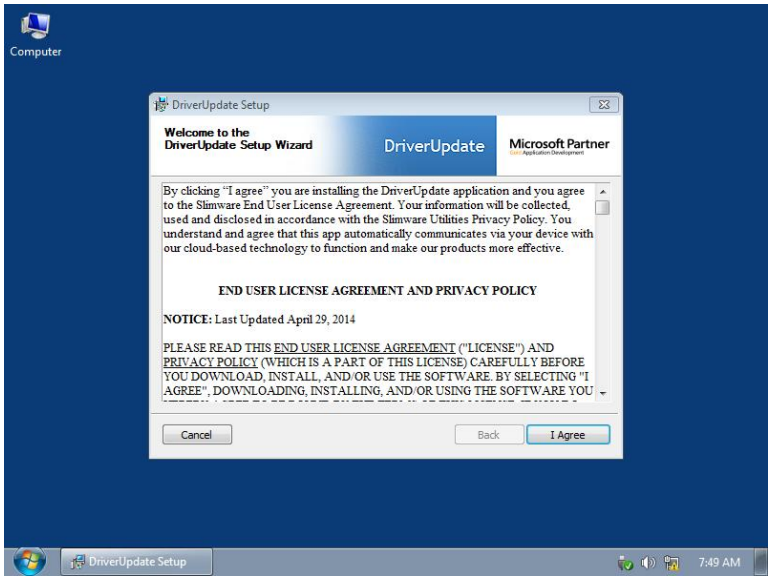
[+] Thawte Timestamping CA	
Status	NoError ✔
Start Date	1997-01-01 02:00:00
End Date	2021-01-01 01:59:59
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Key Identifier	undefined
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	undefined
Extended Usage	undefined

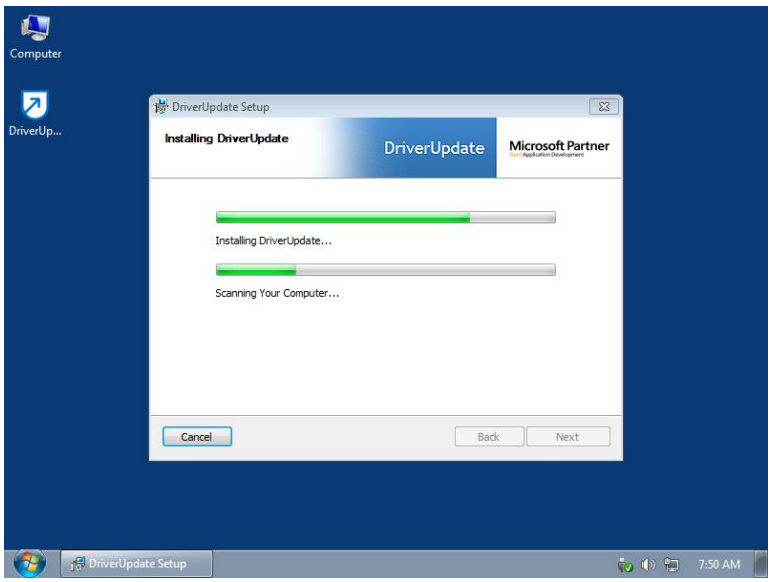
SCREENSHOTS

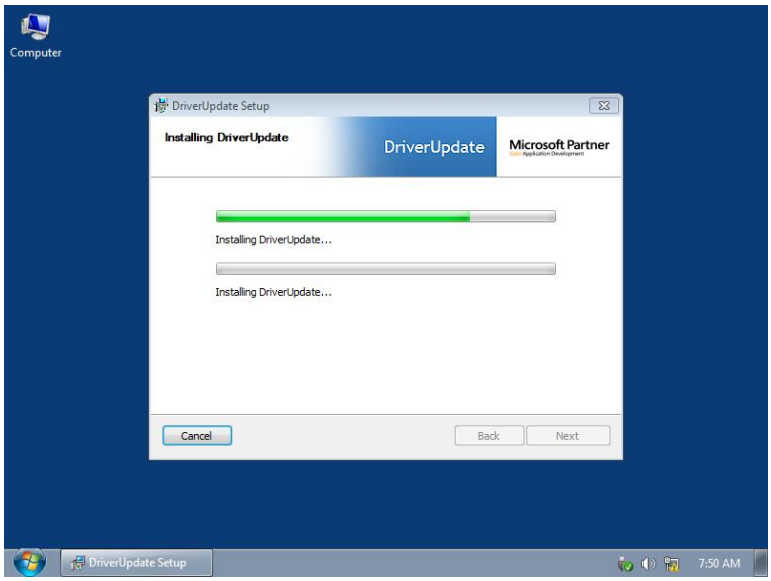


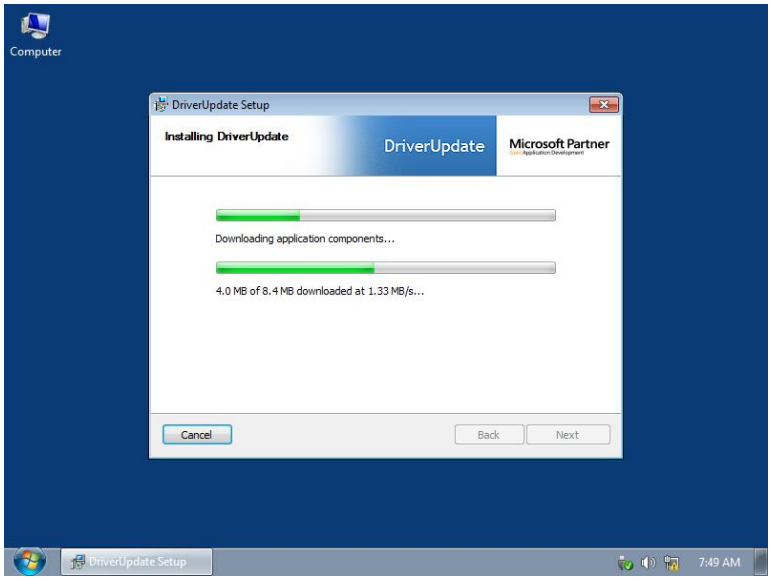


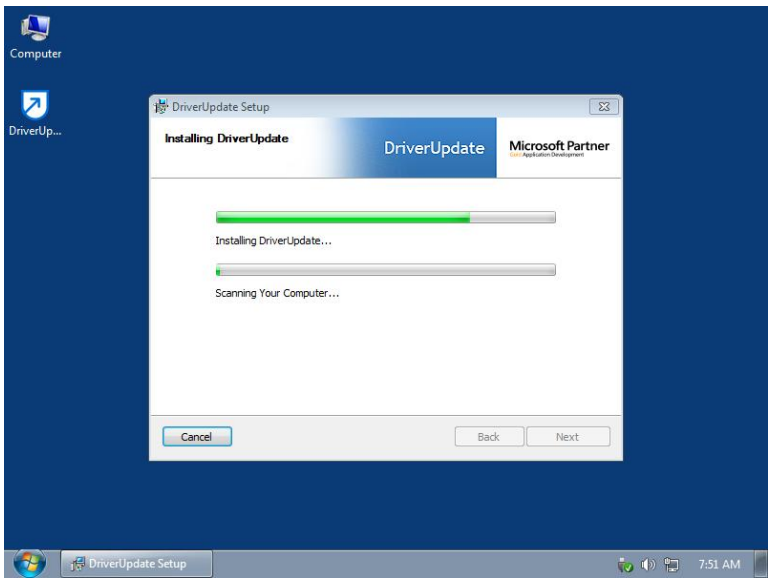

Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Scanning Your Computer...
Cancel
Back
Next
DriverUpdate Setup
7:50 AM

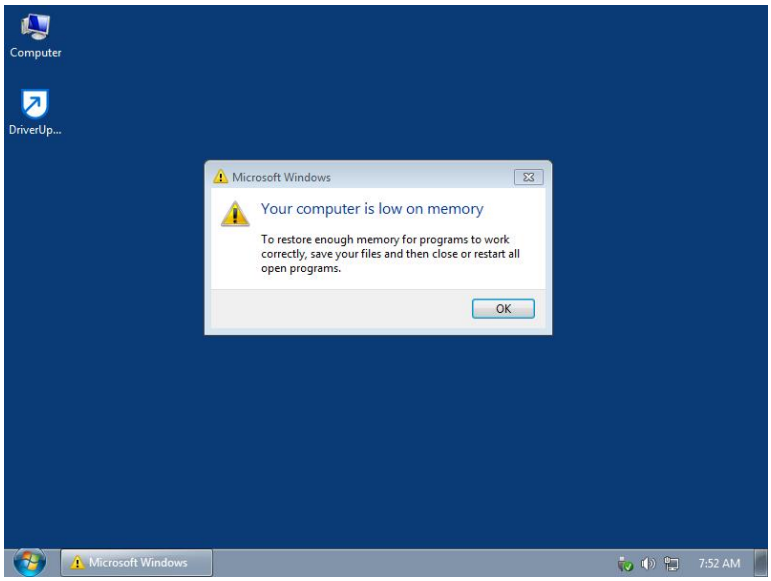

Computer
DriverUpdate Setup
Welcome to the
DriverUpdate Setup Wizard
DriverUpdate
Microsoft Partner
By clicking "I agree" you are installing the DriverUpdate application and you agree to the Slimware End User License Agreement. Your information will be collected, used and disclosed in accordance with 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
7:49 AM

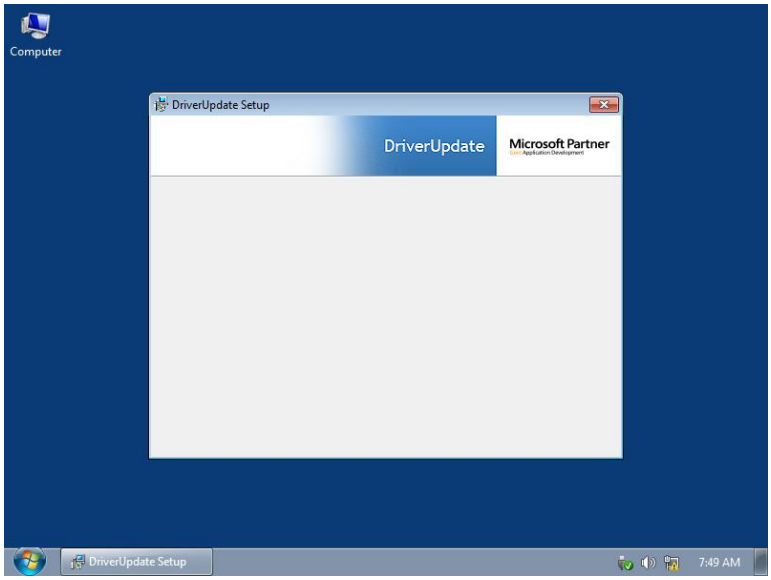

Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Scanning Your Computer...
Cancel
Back
Next
DriverUpdate Setup
7:50 AM


Computer
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Installing DriverUpdate...
Cancel
Back
Next
DriverUpdate Setup
7:50 AM

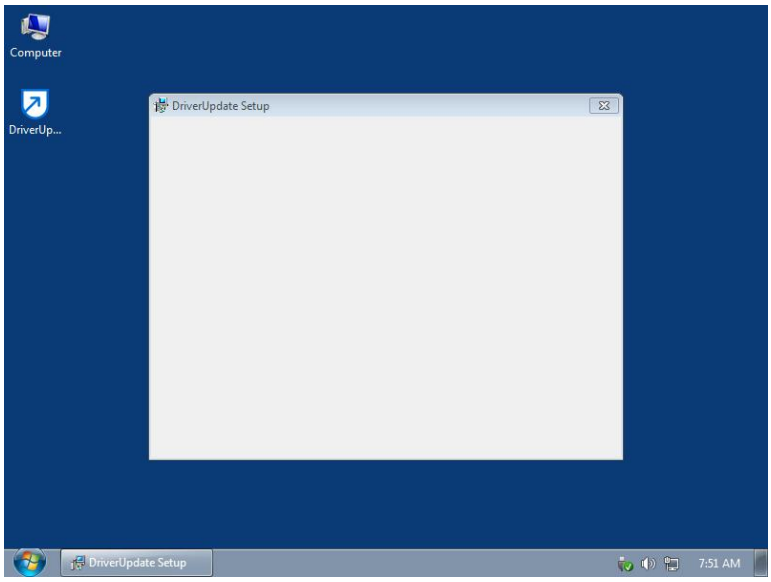

Computer
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Downloading application components...
4.0 MB of 8.4 MB downloaded at 1.33 MB/s...
Cancel
Back
Next
DriverUpdate Setup
7:49 AM

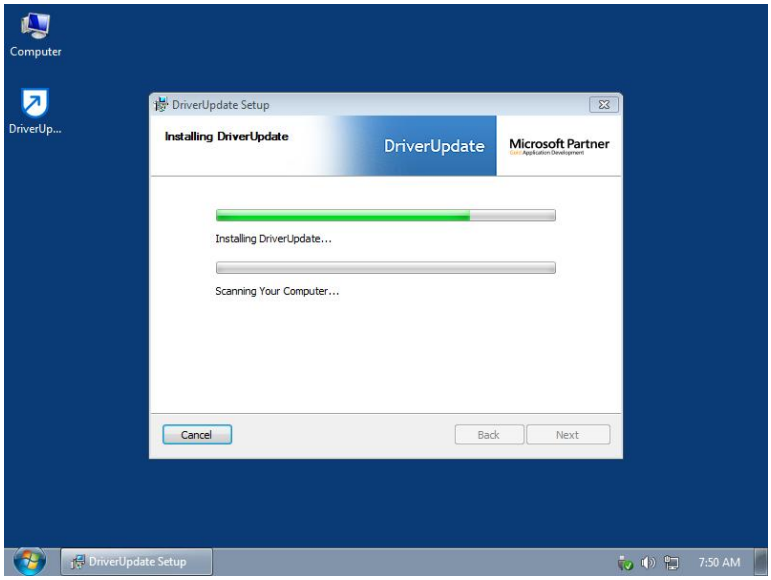

Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Scanning Your Computer...
Cancel
Back
Next
DriverUpdate Setup
7:51 AM

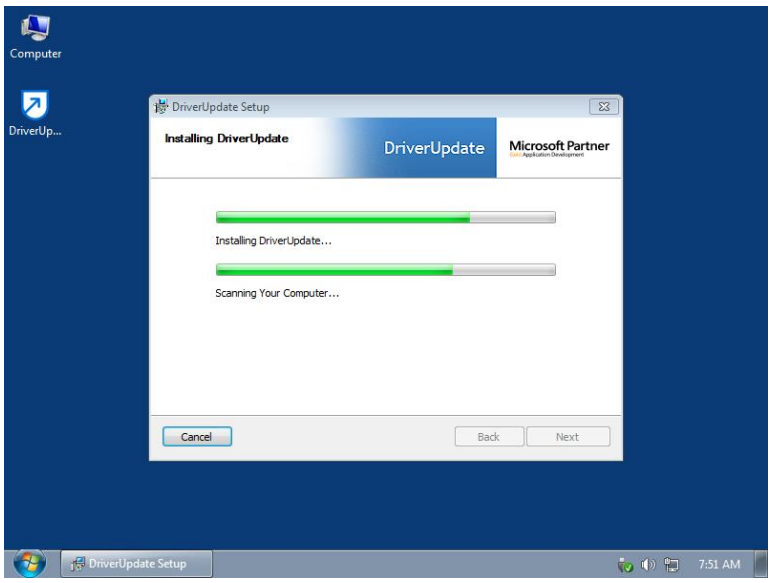

Computer
DriverUp...
Microsoft Windows
Your computer is low on memory
To restore enough memory for programs to work correctly, save your files and then close or restart all open programs.
OK
Microsoft Windows
7:52 AM

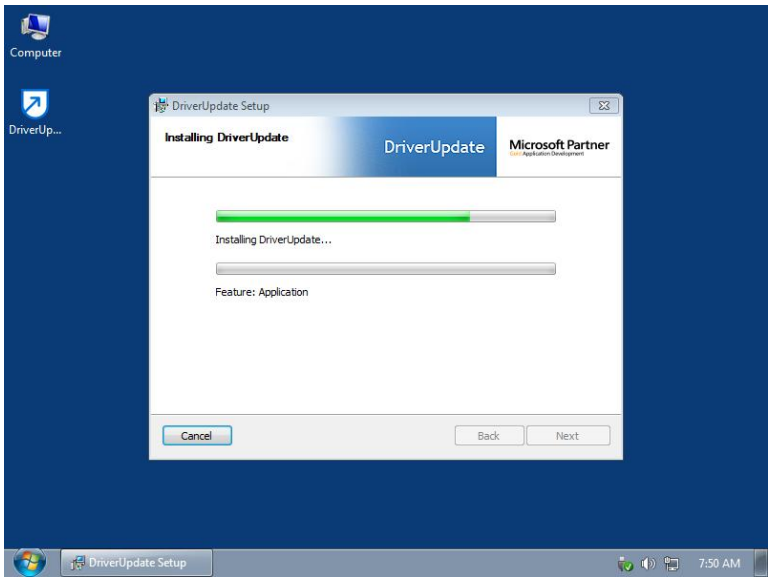

Computer
DriverUpdate Setup
DriverUpdate
Microsoft Partner
DriverUpdate Setup
7:49 AM

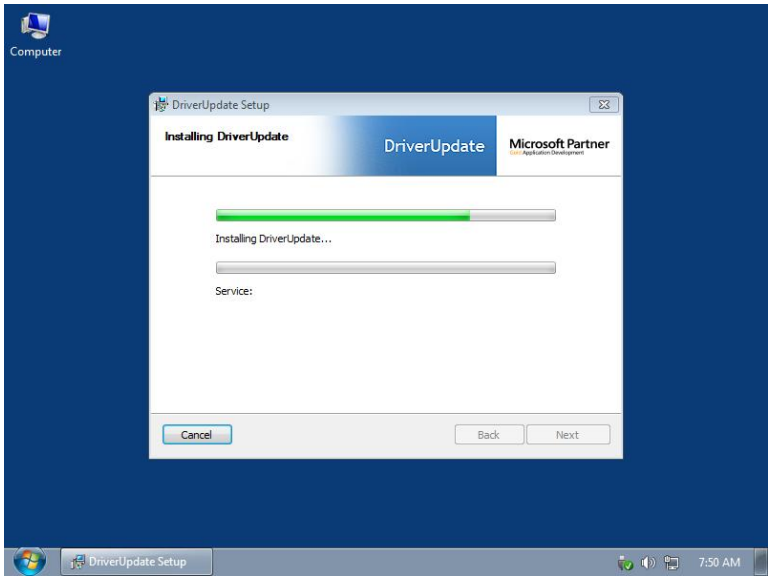

Computer
7:49 AM

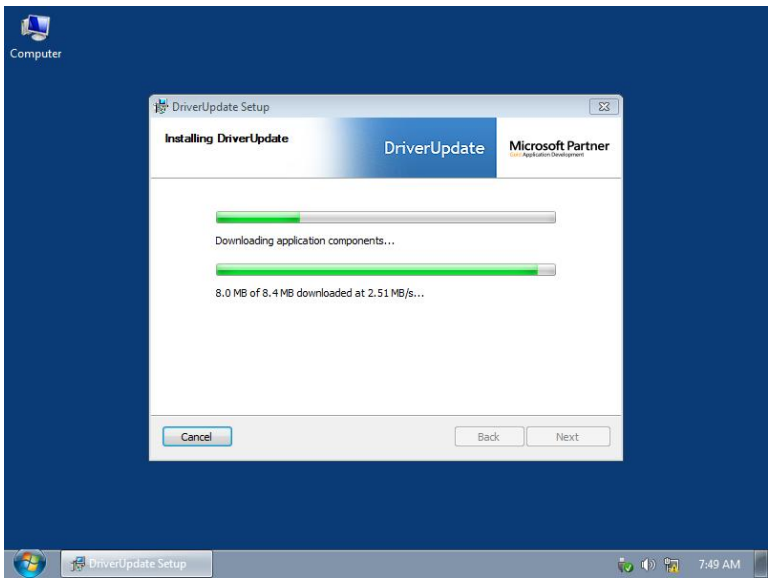

Computer
DriverUp...
DriverUpdate Setup
DriverUpdate Setup
7:51 AM

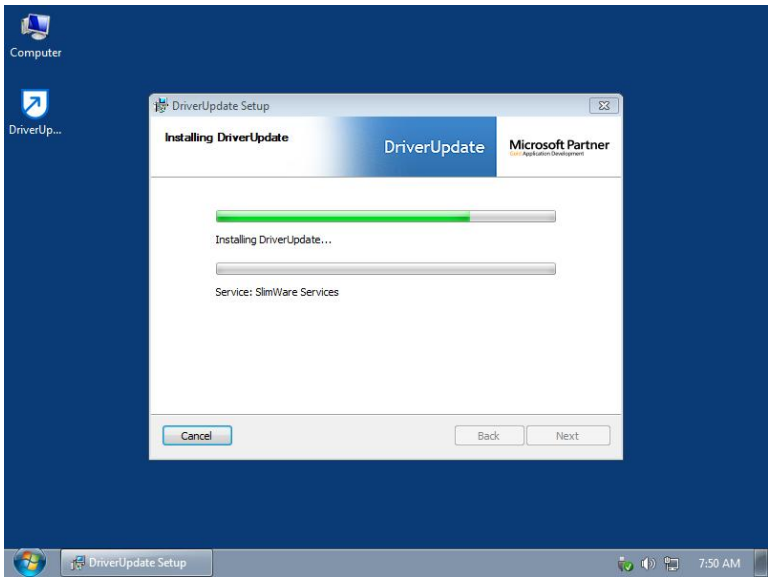

Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Scanning Your Computer...
Cancel
Back
Next
DriverUpdate Setup
7:50 AM

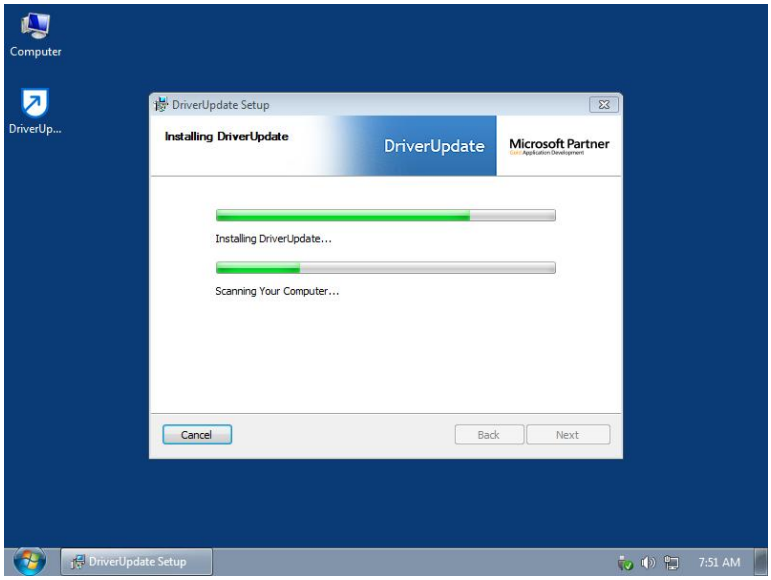

Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Scanning Your Computer...
Cancel
Back
Next
DriverUpdate Setup
7:51 AM

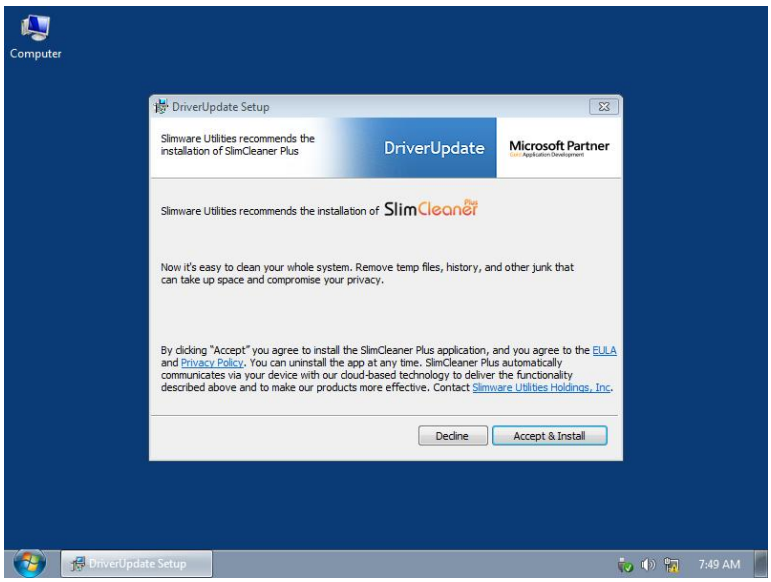

Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Feature: Application
Cancel
Back
Next
DriverUpdate Setup
7:50 AM


Computer
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Service:
Cancel
Back
Next
DriverUpdate Setup
7:50 AM


Computer
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Downloading application components...
8.0 MB of 8.4 MB downloaded at 2.51 MB/s...
Cancel
Back
Next
DriverUpdate Setup
7:49 AM


Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Service: SlimWare Services
Cancel
Back
Next
DriverUpdate Setup
7:50 AM


Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Scanning Your Computer...
Cancel
Back
Next
DriverUpdate Setup
7:51 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
7:49 AM


Computer
DriverUp...
7:51 AM