VALKYRIE COMODO

Summary

File Name: None

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

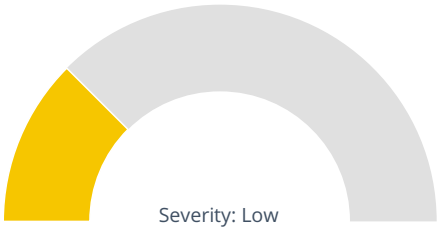
SHA1: 411c2a9901a0c1fe105dfa5e486cdc420bb3f145

MD5: 58adb00645d0cb56306a81935e854733

PUA

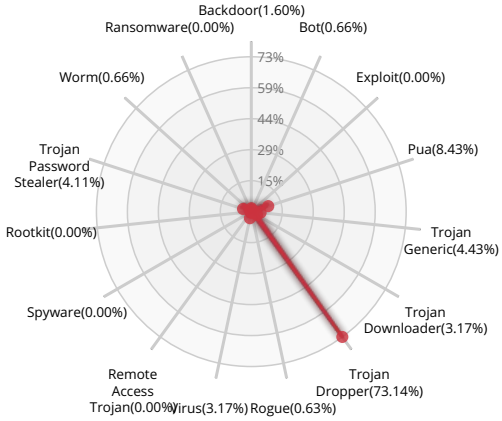
Valkyrie Final Verdict

DETECTION SECTION

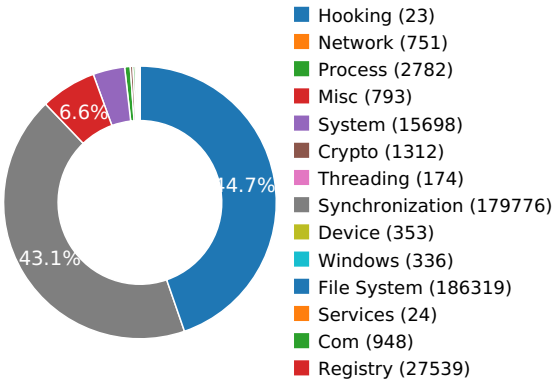


Verdict: PUA

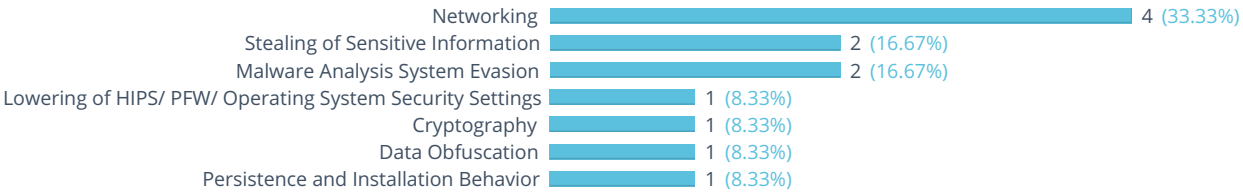
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

NETWORKING

Attempts to connect to a dead IP:Port (11 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
Collects information about installed applications	Show sources

DATA OBFUSCATION

Drops a binary and executes it	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Created a service that was not started	Show sources

MALWARE ANALYSIS SYSTEM EVASION

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

VALKYRIE COMODO

Behavior Graph

01:48:39 **01:50:10** **01:51:40**

PID 2188

01:48:39 Create Process — The malicious file created a child process as 411c2a9901a0c1fe105dfa5e486cdc420bb3f145.exe **(PPID 2076)**

- 01:48:39 / 01:49:07 ConnectEx **[10 times]**
- 01:49:07 Create Process
- 01:49:15 Create Process
- 01:49:18 Create Process

PID 2748

01:49:11 Create Process — The malicious file created a child process as DriverUpdate.exe **(PPID 2188)**

- 01:49:23 NtDelayExecution
- 01:50:59 InternetOpenW
- 01:51:02 ConnectEx
- 01:51:02 InternetOpenW
- 01:51:07 RegQueryValueExW
- 01:51:07 RegOpenKeyExW
- 01:51:07 / 01:51:07 RegQueryValueExW **[92 times]**

PID 2844

01:49:21 Create Process — The malicious file created a child process as scp78E5.tmp.exe **(PPID 2188)**

- 01:49:25 / 01:49:37 ConnectEx **[4 times]**
- 01:49:39 Create Process

PID 2316

01:49:46 Create Process — The malicious file created a child process as SlimCleanerPlus_en-US_x64_Silent.exe **(PPID 2844)**

PID 2260

01:49:25 Create Process — The malicious file created a child process as DriverUpdate.exe **(PPID 2188)**

- 01:50:54 ConnectEx

PID 580

01:49:18 Create Process — The malicious file created a child process as svchost.exe **(PPID 456)**

- 01:49:30 Create Process
- 01:50:02 Create Process
- 01:51:40 Create Process

PID 2800

01:49:35 Create Process — The malicious file created a child process as WmiPrvSE.exe **(PPID 580)**

- 01:49:35 NtDelayExecution
- 01:50:47 RegQueryValueExW

VALKYRIE COMODO

PID 1336

01:50:14	Create Process	The malicious file created a child process as dllhost.exe **(PPID 580)**

PID 1440

01:51:34	Create Process	The malicious file created a child process as unsecapp.exe **(PPID 580)**

PID 1948

01:49:24	Create Process	The malicious file created a child process as svchost.exe **(PPID 456)**

01:49:26	RegOpenKeyExW

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\411c2a9901a0c1fe105dfa5e486cdc420bb3f145.exe.2.Manifest
C:\Users\user\AppData\Local\Temp\411c2a9901a0c1fe105dfa5e486cdc420bb3f145.exe.3.Manifest
C:\Users\user\AppData\Local\Temp\411c2a9901a0c1fe105dfa5e486cdc420bb3f145.exe.Config
C:\Users\user\AppData\Local\Temp\411c2a9901a0c1fe105dfa5e486cdc420bb3f145.exe
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\411c2a9901a0c1fe105dfa5e486cdc420bb3f145.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\swu683A.tmp
C:\
C:\Users\user\AppData\Local\Temp\swu683A.tmp.msi
C:\Users\user\AppData\Local\Temp\scp78E5.tmp
C:\Users\user\AppData\Local\Temp\scp78E5.tmp.exe
C:\Windows\System32\p2pcollab.dll
C:\Windows\System32\qagentrt.dll
C:\Windows\System32\dnsapi.dll
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:\Users\Public\Documents\Downloaded Installers
C:\Users\Public\Documents\Downloaded Installers\{055C7DA5-A1F5-41FB-932C-82474ED3487A}
C:\Users\Public\Documents\Downloaded Installers\{055C7DA5-A1F5-41FB-932C-82474ED3487A}\setup.msi
C:\Users\user\AppData\Local\Temp\
A:
B:
F:
G:
H:
I:
J:

K:
L:
M:
N:
O:
P:
Q:
R:
S:

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\Windows\CurrentVersion\Internet Settings\WinHttp\Tracing\Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ShareCredsWithWinHttp
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\DisableBranchCache
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_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\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollInset
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\DragDelay
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\DragMinDist
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollDelay
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollInterval
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arabic Transparent
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arabic Transparent Bold
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arabic Transparent,0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arabic Transparent Bold,0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Helvetica
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arial Baltic,186
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arial CE,238
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arial CYR,204
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arial Greek,161
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arial TUR,162
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Courier New Baltic,186
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Courier New CE,238
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Courier New CYR,204
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Courier New Greek,161
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Courier New TUR,162
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Times
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Times New Roman Baltic,186
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Times New Roman CE,238
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Times New Roman CYR,204
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Times New Roman Greek,161
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Times New Roman TUR,162
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Tahoma Armenian
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Helv
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Tms Rmn
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\David Transparent
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Miriam Transparent
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Fixed Miriam Transparent
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Rod Transparent
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\FangSong_GB2312
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\KaiTi_GB2312
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Certificate\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Certificate\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Initialization\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Initialization\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Message\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Message\{00AAC56B-CD44-11D0-8CC2-00C04FC295EE}\$Function

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\swu683A.tmp
C:\Users\user\AppData\Local\Temp\swu683A.tmp.msi
C:\Users\user\AppData\Local\Temp\scp78E5.tmp
C:\Users\user\AppData\Local\Temp\scp78E5.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\{055C7DA5-A1F5-41FB-932C-82474ED3487A}\setup.msi
C:\Users\user\AppData\Local\Temp\MSIc9283.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\2018-10-20 12-38-29 0.log
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\SWDUMon.inf
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\SWDUMon.sys
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\SWDUMon.cat
C:\Windows\inf\setupapi.app.log
C:\Windows\sysnative\drivers\SET2475.tmp
C:\Windows\sysnative\drivers\SWDUMon.sys
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\supdates.db
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\supdates.db-journal
C:\Users\user\AppData\Local\Temp\SWI277.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
\??\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
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Logs\2018-10-20 12-38-38 0.log
\??\WMIDataDevice
\??\PIPE\lsarpc
\??\PIPE\srvsvc
\??\PIPE\wkssvc
C:\Users\user\AppData\Local\Temp\SIOUT13346281\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\MSIbda57.LOG

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
kernel32.dll.IsWow64Process
shlwapi.dll.StrRChrA
winhttp.dll.WinHttpGetIEProxyConfigForCurrentUser
oleaut32.dll.#8
oleaut32.dll.#12
comctl32.dll.InitCommonControlsEx
dwmapi.dll.DwmIsCompositionEnabled
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
shlwapi.dll.StrCmpNW
oleaut32.dll.#4
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
gdi32.dll.GetTextFaceAliasW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey

advapi32.dll.RegQueryValueExW
oleaut32.dll.#6
ole32.dll.CoInitializeEx
advapi32.dll.RegDeleteTreeA
advapi32.dll.RegDeleteTreeW
ole32.dll.CoTaskMemAlloc
ole32.dll.StringFromIID
nsi.dll.NsiAllocateAndGetTable
gdi32.dll.GetFontAssocStatus
cfgmgr32.dll.CM_Open_Class_Key_ExW
iphlpapi.dll.ConvertInterfaceGuidToLuid
iphlpapi.dll.GetIfEntry2
advapi32.dll.RegQueryValueExA
advapi32.dll.RegEnumKeyExW
iphlpapi.dll.GetIpForwardTable2
iphlpapi.dll.GetIpNetEntry2
iphlpapi.dll.FreeMibTable
ole32.dll.CoTaskMemFree
nsi.dll.NsiFreeTable
oleaut32.dll.#9
user32.dll.GetSystemMetrics
user32.dll.MonitorFromWindow
user32.dll.MonitorFromRect
user32.dll.MonitorFromPoint
user32.dll.EnumDisplayDevicesW
user32.dll.GetMonitorInfoW
ole32.dll.CoUninitialize
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoRevokeInitializeSpy
oleaut32.dll.#500
shlwapi.dll.#153
winhttp.dll.WinHttpDetectAutoProxyConfigUrl
ws2_32.dll.GetAddrInfoW
comctl32.dll.RegisterClassNameW

ws2_32.dll.getaddrinfo
uxtheme.dll.EnableThemeDialogTexture
uxtheme.dll.OpenThemeData
uxtheme.dll.GetThemeBool
comctl32.dll.HIMAGELIST_QueryInterface

DELETED FILES

C:\Users\user\AppData\Local\Temp\swu683A.tmp
C:\Users\user\AppData\Local\Temp\swu683A.tmp.msi
C:\Users\user\AppData\Local\Temp\scp78E5.tmp
C:\Users\user\AppData\Local\Temp\scp78E5.tmp.exe
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\settings.db-wal
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\settings.db-journal
C:\Windows\sysnative\drivers\SET2475.tmp
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\supdates.db-wal
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\supdates.db-journal
C:\Users\user\AppData\Local\Temp\SlimCleanerPlus_en-US_x64_Silent.exe
C:\Users\user\AppData\Local\Temp\SWI277.tmp

DELETED REGISTRY KEYS

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

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32
HKEY_LOCAL_MACHINE\SOFTWARE\SlimWare Utilities Inc
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\Registration
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\MachineID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\Registration\InstallationID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\Tracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\Tracing\Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ShareCredsWithWinHttp
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\DisableBranchCache
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Internet Settings\Wpad
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00
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\CTF\Compatibility\411c2a9901a0c1fe105dfa5e486cdc420bb3f145.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
HKEY_CURRENT_USER
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollInset
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\DragDelay
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\DragMinDist
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollDelay
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\ScrollInterval
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arabic Transparent
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arabic Transparent Bold
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arabic Transparent,0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arabic Transparent Bold,0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Helvetica
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arial Baltic,186
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arial CE,238
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arial CYR,204
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arial Greek,161
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Arial TUR,162
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Courier New Baltic,186
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Courier New CE,238
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Courier New CYR,204

EXECUTED COMMANDS

"C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe" -installscan
"C:\Users\user\AppData\Local\Temp\scp78E5.tmp.exe" SI_LAUNCH=onreboot SI_MODE=toaster SI_DELAY=5 @P2_ORIGIN=^SW1^xdm111 @P2=^SW2^xdm633^^ @UL_STUBID=651bb31e-539c-4290-9642-c7c4585dca22

"C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe" -installresults
C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
C:\Windows\system32\wbem\unsecapp.exe -Embedding
"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\411c2a9901a0c1fe105dfa5e486cdc420bb3f145.exe.2.Manifest
C:\Users\user\AppData\Local\Temp\411c2a9901a0c1fe105dfa5e486cdc420bb3f145.exe.3.Manifest
C:\Users\user\AppData\Local\Temp\411c2a9901a0c1fe105dfa5e486cdc420bb3f145.exe.Config
C:\Users\user\AppData\Local\Temp\411c2a9901a0c1fe105dfa5e486cdc420bb3f145.exe
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\swu683A.tmp
C:\Users\user\AppData\Local\Temp\scp78E5.tmp
C:\Users\user\AppData\Local\Temp\swu683A.tmp.msi
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\4FDDCB9326035346 77ECAE8C7D0FD914FD443E83
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\{055C7DA5-A1F5-41FB-932C-82474ED3487A}\setup.msi
C:\Windows\System32\msimsg.dll
C:\Windows\SysWOW64\shell32.dll
C:
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\settings.db
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\settings.db-journal
C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe.2.Manifest
C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe.3.Manifest
C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe.Config
C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe
C:\Program Files (x86)\DriverUpdate\DriverUpdate.exe.1000.Manifest
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\ignores.dat
C:\Windows\System32\tzres.dll
C:\Windows\inf\netrasa.inf
C:\Windows\System32\p2pcollab.dll
C:\Windows\System32\en-US\dnsapi.DLL.mui
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\SWDUMon.inf
C:\Windows\inf\setupapi.app.log
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\SWDUMon.sys
C:\Windows\sysnative\drivers\SET2475.tmp
C:\Windows\inf\keyboard.inf
C:\Windows\inf\blbdrive.inf

C:\Windows\inf\mshdc.inf
C:\Windows\inf\msports.inf
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\rupdates.db
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\supdates.db
C:\Windows\inf\compositebus.inf
C:\Users\user\AppData\Local\SlimWare Utilities Inc\DriverUpdate\supdates.db-journal
C:\Windows\inf\machine.inf
C:\Windows\inf\battery.inf
C:\Windows\inf\disk.inf
C:\Windows\inf\msmouse.inf
C:\Windows\inf\acpi.inf
C:\Windows\inf\umbus.inf
C:\Windows\inf\netsstpa.inf

MUTEXES

DBWinMutex
{042B0D65-EF5B-4E3F-ADFF-86C726E4F053}
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Global\MSILOG_9c9164f41d46838GOL.3829cISM_pmeT_lacoL_ataDppA_resu_sresU_:C
Global_MSIExecute
SlimWare Utilities, Inc..DriverUpdate
IESQMMUTEX_0_208
Global\MSILOG_bf0e11c01d46838GOL.75adbISM_pmeT_lacoL_ataDppA_resu_sresU_:C

MODIFIED REGISTRY KEYS

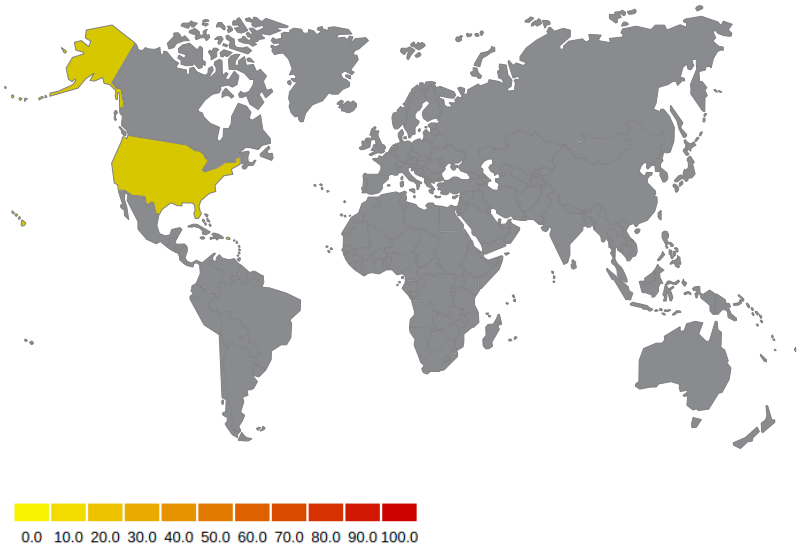
HKEY_LOCAL_MACHINE\SOFTWARE\SlimWare Utilities Inc
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\Registration
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\MachineID
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\GlobalAssocChangedCounter
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\tbInstallationSessionID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\InstallationSessionID
HKEY_CURRENT_USER\SOFTWARE\SlimWare Utilities Inc\DriverUpdate
HKEY_CURRENT_USER\Software\SlimWare Utilities Inc\DriverUpdate\InstallationSessionID

HKEY_CURRENT_USER\Software\SlimWare Utilities Inc\tbInstallationSessionID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\InstallerData
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\InstallerData\browser
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\InstallerData\s2s
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\InstallerData\scanPagePixel
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\InstallerData\userSegments
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\InstallerData\vurl
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\Registration\InstallationID
HKEY_CURRENT_USER\Software\SlimWare Utilities Inc\DriverUpdate\InstallScanUrlParams
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6F\52C64B7E\LanguageList
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6F\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6F\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_LOCAL_MACHINE\SYSTEM\Setup\SetupapiLogStatus\setupapi.app.log
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\SWDUMon\BasePath
HKEY_LOCAL_MACHINE\SOFTWARE\SlimWare Utilities, Inc.\DriverApp\Installed
HKEY_LOCAL_MACHINE\SOFTWARE\SlimWare Utilities, Inc.\DriverApp\Downloaded
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\SlimCleaner Plus\Registration
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_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\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

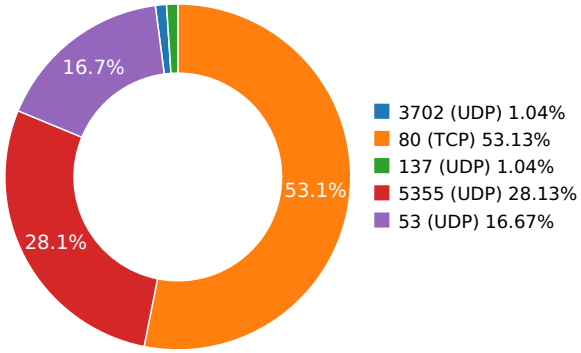
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\ESS\//./root/CIMV2\SCM Event Provider
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
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_LOCAL_MACHINE\SOFTWARE\SlimWare Utilities Inc\DriverUpdate\PNGS
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SlimWare Utilities Inc\DriverUpdate\PNGS\RN

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
	13.33.80.116	United States	16509	Amazon Technologies Inc.	Malware Process
	13.33.80.46	United States	16509	Amazon Technologies Inc.	Malware Process
	151.101.2.133	United States	54113	Fastly	Malware Process
	23.215.131.200	United States	20940	Akamai Technologies, Inc.	OS Process
	23.35.171.27	United States	20940	Akamai Technologies, Inc.	Malware Process
	34.231.33.210	United States	14618	Amazon Technologies Inc.	Malware Process
	52.216.224.226	United States	16509	Amazon Technologies Inc.	Malware Process
	54.231.40.17	United States	16509	Amazon.com, Inc.	Malware Process
trk.slimwareutilities.com	54.175.217.102	United States	14618	Amazon Technologies Inc.	Malware Process
stats.slimwareutilities.com	52.216.226.18	United States	16509	Amazon Technologies Inc.	Malware Process
www.slimwareutilities.com	50.17.223.81	United States	14618	Amazon.com, Inc.	Malware Process
stc.slimwareutilities.com	52.20.7.33	United States	14618	Amazon Technologies Inc.	Malware Process
crl.microsoft.com	23.192.125.97	United States	20940	Akamai Technologies, Inc.	OS Process
crl.globalsign.net	151.101.118.133	United States	54113	Fastly	Malware Process
ctldl.windowsupdate.com	72.21.81.240	United States	15133	MCI Communications Servic...	OS Process
download.driverupdate.net	52.85.93.145	United States	16509	Amazon Technologies Inc.	Malware Process
apps-api.slimwareutilities.com	52.44.174.33	United States	14618	Amazon Technologies Inc.	Malware Process
cdn.slimcleaner.com	52.85.93.5	United States	16509	Amazon Technologies Inc.	Malware Process
sf.symcd.com	23.54.187.27	United States	16625	Akamai Technologies, Inc.	Malware Process
ocsp.verisign.com	23.54.187.27	United States	16625	Akamai Technologies, Inc.	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
www.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	5.97793507576
Path: /installer/init_v2.php **URI:** http://www.slimwareutilities.com/installer/init_v2.php						
stats.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	7.76453208923
Path: /api/flow/action **URI:** http://stats.slimwareutilities.com/api/flow/action						
stats.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	7.79384016991
Path: /api/flow/action **URI:** http://stats.slimwareutilities.com/api/flow/action						
stats.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	7.81218218803
Path: /api/flow/action **URI:** http://stats.slimwareutilities.com/api/flow/action						
stats.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	7.82931613922
Path: /api/flow/action **URI:** http://stats.slimwareutilities.com/api/flow/action						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	8.48067808151
Path: /ulc.php? ev=InstallerInvoked&upl=YToxMjp7czo5OiJ1bF9zdHViaWQiO3M6MzY6IjY1MWJiMzFlLTUzOWMtNDI5MC05NjQyLWM3YzQ1ODVkY2EyMiI7czoxMDoidWxfY29icmFuZCI7czozOiJTVzIiO3M6MTE6InVsX2NhbXBhaWduIjtzOjY6InhkbTYzMyI7czo4OiJ1bF9zdWJpZCI7czozOiI2MzYiO3M6NzoiYWRHcm91cCI7czo0OiI0MTY2IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjEyOiJ1c2VyU2VnbWVudHMiO086ODoic3RkQ2xhc3MiOjE6e3M6MTI6IlBob25lU3VwcG9ydCI7TzozOiJzdGRDbGFzcyI6Mjp7czoxMzoiU3VwcG9ydFZlbmRvciI7czo4OiJTbGltV2FyZSI7czoxNzoiU3VwcG9ydE51bWJlclR5cGUiO3M6MTA6IkFjdGl2YXRpb24iO319czoxMToiYnJvd3NlclR5cGUiO3M6MTA6IkNocm9tZSI7czoxMDoiYnJvd3NlclZlcnNpb24iO3M6ODoiMTQuMTQzOTMiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czo0OiIxMC4wIjt9&machineId=1C3D66D7-076C-41B9-AC2A-46C332DE0DA0 **URI:** http://trk.slimwareutilities.com/ulc.php? ev=InstallerInvoked&upl=YToxMjp7czo5OiJ1bF9zdHViaWQiO3M6MzY6IjY1MWJiMzFlLTUzOWMtNDI5MC05NjQyLWM3YzQ1ODVkY2EyMiI7czoxMDoidWxfY29icmFuZCI7czozOiJTVzIiO3M6MTE6InVsX2NhbXBhaWduIjtzOjY6InhkbTYzMyI7czo4OiJ1bF9zdWJpZCI7czozOiI2MzYiO3M6NzoiYWRHcm91cCI7czo0OiI0MTY2IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjEyOiJ1c2VyU2VnbWVudHMiO086ODoic3RkQ2xhc3MiOjE6e3M6MTI6IlBob25lU3VwcG9ydCI7TzozOiJzdGRDbGFzcyI6Mjp7czoxMzoiU3VwcG9ydFZlbmRvciI7czo4OiJTbGltV2FyZSI7czoxNzoiU3VwcG9ydE51bWJlclR5cGUiO3M6MTA6IkFjdGl2YXRpb24iO319czoxMToiYnJvd3NlclR5cGUiO3M6MTA6IkNocm9tZSI7czoxMDoiYnJvd3NlclZlcnNpb24iO3M6ODoiMTQuMTQzOTMiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czo0OiIxMC4wIjt9&machineId=1C3D66D7-076C-41B9-AC2A-46C332DE0DA0						
download.driverupdate.net	80	GET	1.1	SLIMHTTP/1.1	1	8.63656711578
Path: /en/DriverUpdate-setup.msi.bz2 **URI:** http://download.driverupdate.net/en/DriverUpdate-setup.msi.bz2						
stats.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	9.82247614861
Path: /api/flow/action **URI:** http://stats.slimwareutilities.com/api/flow/action						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	10.3137052059

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /ulc.php?ev=InstallerAccepted&upl=YToxMjp7czo5OiJ1bF9zdHViaWQiO3M6MzY6IjY1MWJiMzFlLTUzOWMtNDI5MC05NjQyLWM3YzQ1ODVkY2EyMiI7czoxMDoidWxfY29icmFuZCI7czozOiJTVzIiO3M6MTE6InVsX2NhbXBhaWduIjtzOjY6InhkbTYzMyI7czo4OiJ1bF9zdWJpZCI7czozOiI2MzYiO3M6NzoiYWRHcm91cCI7czo0OiI0MTY2IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjEyOiJ1c2VyU2VnbWVudHMiO086ODoic3RkQ2xhc3MiOjE6e3M6MTI6IlBob25lU3VwcG9ydCI7czo4OiJzdGRDbGFzcyI6Mjp7czoxMzoiU3VwcG9ydFZlbmRvciI7czo4OiJTbGltV2FyZSI7czoxNzoiU3VwcG9ydCI7czo4OiJTbGltV2FyZSI7czoxMDoiYnJvd3NlclR5cGUiO3M6MTA6IkFuZHJvaWQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czo0OiIxMC4wIjt9&machineId=1C3D66D7-076C-41B9-AC2A-46C332DE0DA0 **URI:** http://trk.slimwareutilities.com/ulc.php?ev=InstallerAccepted&upl=YToxMjp7czo5OiJ1bF9zdHViaWQiO3M6MzY6IjY1MWJiMzFlLTUzOWMtNDI5MC05NjQyLWM3YzQ1ODVkY2EyMiI7czoxMDoidWxfY29icmFuZCI7czozOiJTVzIiO3M6MTE6InVsX2NhbXBhaWduIjtzOjY6InhkbTYzMyI7czo4OiJ1bF9zdWJpZCI7czozOiI2MzYiO3M6NzoiYWRHcm91cCI7czo0OiI0MTY2IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjEyOiJ1c2VyU2VnbWVudHMiO086ODoic3RkQ2xhc3MiOjE6e3M6MTI6IlBob25lU3VwcG9ydCI7czo4OiJzdGRDbGFzcyI6Mjp7czoxMzoiU3VwcG9ydFZlbmRvciI7czo4OiJTbGltV2FyZSI7czoxNzoiU3VwcG9ydCI7czo4OiJTbGltV2FyZSI7czoxMDoiYnJvd3NlclR5cGUiO3M6MTA6IkFuZHJvaWQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czo0OiIxMC4wIjt9&machineId=1C3D66D7-076C-41B9-AC2A-46C332DE0DA0						
cdn.slimcleaner.com	80	GET	1.1	SLIMHTTP/1.1	1	12.9094910622
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	18.6425011158
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?caa90e7fe06b5907 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?caa90e7fe06b5907						
ocsp.verisign.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	24.0406351089
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	29.3270590305
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	33.8816361427
Path: /ulc.php?ev=InstallerFinished&upl=YToxMjp7czo5OiJ1bF9zdHViaWQiO3M6MzY6IjY1MWJiMzFlLTUzOWMtNDI5MC05NjQyLWM3YzQ1ODVkY2EyMiI7czoxMDoidWxfY29icmFuZCI7czozOiJTVzIiO3M6MTE6InVsX2NhbXBhaWduIjtzOjY6InhkTYzMyI7czo4OiJ1bF9zdWJpZCI7czozOiI2MzYiO3M6NzoiYWRHcm91cCI7czo0OiI0MTY2IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjEyOiJ1c2VyU2VnbWVudHMiO086ODoic3RkQ2xhc3MiOjE6e3M6MTI6IlBob25lU3VwcG9ydCI7czo4OiJzdGRDbGFzcyI6Mjp7czoxMzoiU3VwcG9ydFZlbmRvciI7czo4OiJTbGltV2FyZSI7czoxNzoiU3VwcG9ydCI7czo4OiJTbGltV2FyZSI7czoxMDoiYnJvd3NlclR5cGUiO3M6MTA6IkFuZHJvaWQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czo0OiIxMC4wIjt9&machineId=1C3D66D7-076C-41B9-AC2A-46C332DE0DA0&installId=52F619EC-34A1-4F9B-9871-8DC5C253D44C **URI:** http://trk.slimwareutilities.com/ulc.php?ev=InstallerFinished&upl=YToxMjp7czo5OiJ1bF9zdHViaWQiO3M6MzY6IjY1MWJiMzFlLTUzOWMtNDI5MC05NjQyLWM3YzQ1ODVkY2EyMiI7czoxMDoidWxfY29icmFuZCI7czozOiJTVzIiO3M6MTE6InVsX2NhbXBhaWduIjtzOjY6InhkTYzMyI7czo4OiJ1bF9zdWJpZCI7czozOiI2MzYiO3M6NzoiYWRHcm91cCI7czo0OiI0MTY2IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjEyOiJ1c2VyU2VnbWVudHMiO086ODoic3RkQ2xhc3MiOjE6e3M6MTI6IlBob25lU3VwcG9ydCI7czo4OiJzdGRDbGFzcyI6Mjp7czoxMzoiU3VwcG9ydFZlbmRvciI7czo4OiJTbGltV2FyZSI7czoxNzoiU3VwcG9ydCI7czo4OiJTbGltV2FyZSI7czoxMDoiYnJvd3NlclR5cGUiO3M6MTA6IkFuZHJvaWQiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czo0OiIxMC4wIjt9&machineId=1C3D66D7-076C-41B9-AC2A-46C332DE0DA0&installId=52F619EC-34A1-4F9B-9871-8DC5C253D44C						
stats.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	33.9617540836
Path: /api/flow/action **URI:** http://stats.slimwareutilities.com/api/flow/action						
stats.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	42.1730670929
Path: /api/flow/action **URI:** http://stats.slimwareutilities.com/api/flow/action						

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
stats.slimwareutilities.com	80	POST	1.1	Mozilla/4.0 (compatible; W...	1	44.4034221172
Path: /api/flow/action **URI:** http://stats.slimwareutilities.com/api/flow/action						
stc.slimwareutilities.com	80	GET	1.1	SilentDownloader/2.4.1	1	45.3612411022
Path: /gettrack?product=SW1&p2=%5ESW2%5Exdm633%5E%5E&secondOfferOrigin=%5ESW1%5Exdm111&ul_stubid=651bb31e-539c-4290-9642-c7c4585dca22 **URI:** http://stc.slimwareutilities.com/gettrack?product=SW1&p2=%5ESW2%5Exdm633%5E%5E&secondOfferOrigin=%5ESW1%5Exdm111&ul_stubid=651bb31e-539c-4290-9642-c7c4585dca22						
cdn.slimcleaner.com	80	GET	1.1	SilentDownloader/2.4.1	1	45.5479290485
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	45.5486860275
Path: /ulc.php?ev=InstallerInvoked&platformOSVersion=6.1&secondOfferOrigin=%5ESW1%5Exdm111&ul_stubid=651bb31e-539c-4290-9642-c7c4585dca22&p2=%5ESW2%5Exdm633%5E%5E&installer=SD0&product=SW1&installerVersion=2.4.1&machineId=1C3D66D7-076C-41B9-AC2A-46C332DE0DA0&platformOS=Windows&ul_track=SCP077 **URI:** http://trk.slimwareutilities.com/ulc.php?ev=InstallerInvoked&platformOSVersion=6.1&secondOfferOrigin=%5ESW1%5Exdm111&ul_stubid=651bb31e-539c-4290-9642-c7c4585dca22&p2=%5ESW2%5Exdm633%5E%5E&installer=SD0&product=SW1&installerVersion=2.4.1&machineId=1C3D66D7-076C-41B9-AC2A-46C332DE0DA0&platformOS=Windows&ul_track=SCP077						
sf.symcd.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	57.5836369991
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTSqZMG5M8TA9rdzkbCnNwuMAd5VgQUz5mp6nsm9EvJjo%2FX8AUm7%2BPSp50CEDBjs6dAwc39%2BLuebDMa194%3D **URI:** http://sf.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTSqZMG5M8TA9rdzkbCnNwuMAd5VgQUz5mp6nsm9EvJjo%2FX8AUm7%2BPSp50CEDBjs6dAwc39%2BLuebDMa194%3D						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	65.046749115
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	70.6414160728
Path: /pki/crl/products/CodeSignPCA2.crl **URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	76.4966821671
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	83.0204370022
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						
trk.slimwareutilities.com	80	GET	1.1	SilentDownloader/2.4.1	1	86.6168100834
Path: /ulc.php?ev=InstallerFinished&platformOSVersion=6.1&secondOfferOrigin=%5ESW1%5Exdm111&installId=3B6E3FE8-0EE6-46BC-B27A-A1EE8D73C6F7&ul_stubid=651bb31e-539c-4290-9642-c7c4585dca22&p2=%5ESW2%5Exdm633%5E%5E&installer=SD0&product=SW1&installerVersion=2.4.1&machineId=1C3D66D7-076C-41B9-AC2A-46C332DE0DA0&platformOS=Windows&ul_track=SCP077 **URI:** http://trk.slimwareutilities.com/ulc.php?ev=InstallerFinished&platformOSVersion=6.1&secondOfferOrigin=%5ESW1%5Exdm111&installId=3B6E3FE8-0EE6-46BC-B27A-A1EE8D73C6F7&ul_stubid=651bb31e-539c-4290-9642-c7c4585dca22&p2=%5ESW2%5Exdm633%5E%5E&installer=SD0&product=SW1&installerVersion=2.4.1&machineId=1C3D66D7-076C-41B9-AC2A-46C332DE0DA0&platformOS=Windows&ul_track=SCP077						
apps-api.slimwareutilities.com	80	POST	1.1	PHP.Serialize	2	133.790081024

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /v1/AutoActivate **URI:** http://apps-api.slimwareutilities.com/v1/AutoActivate						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	134.102061987
Path: /ulc.php?ev=Startup&installId=52F619EC-34A1-4F9B-9871-8DC5C253D44C&browser=chrome&productVersion=2.7.11.0&product=SW2&hasUI=yes&vurl=4166&s2s=NjM2fDcyODEzfFVTfDQ0fDF8fHx8fA%7C%7C%7C636&up=YToxMjp7czo5OiJ1bF9zdHViaWQiO3M6MzY6IjY1MWJiMzFlLTUzOWMtNDI5MC05NjQyLWM3YzQ1ODVkY2EyMiI7czoxMDoidWxfY29icmFuZCI7czozOiJTVzIiO3M6MTE6InVsX2NhbXBhaWduIjtzOjY6InhkbTYzMyI7czo4OiJ1bF9zdWJpZCI7czozOiI2MzYiO3M6NzoiYWRHcm91cCI7czo0OiI0MTY2IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjEyOiJ1c2VyU2VnbWVudHMiO086ODoic3RkQ2xhc3MiOjE6e3M6MTI6IlBob25lU3VwcG9ydCI7Tzo4OiJzdGRDbGFzcyI6Mjp7czoxMzoiU3VwcG9ydFZlbmRvciI7czo4OiJTbGltV2FyZSI7czoxNzoiU3VwcG9ydE51bWJlclR5cGUiO3M6MTA6IkFjdGl2YXRpb24iO319czoxMToiYnJvd3NlclR5cGUiO3M6NDoiRWRnZSI7czoxNDoiYnJvd3NlclZlcnNpb24iO3M6ODoiMTQuMTQzOTMiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czo0OiIxMC4wIjt9&machineId=1C3D66D7-076C-41B9-AC2A-46C332DE0DA0&isRegistered=no&userSegments=O%3A8%3A%22stdClass%22%3A1%3A%7Bs%3A12%3A%22PhoneSupport%22%3BO%3A8%3A%22stdClass%22%3A2%3A%7Bs%3A13%3A%22SupportVendor%22%3Bs%3A8%3A%22SlimWare%22%3Bs%3A17%3A%22SupportNumberType%22%3Bs%3A10%3A%22Activation%22%3B%7D%7D&eventSource=SYSTEM&scanPagePixel=%7B%22parameters%22%3A%7B%22slimprid%22%3A%22%5ESW2%5Exdm633%22%2C%22s2s%22%3A%22NjM2fDcyODEzfFVTfDQ0fDF8fHx8fA%7C%7C%7C636%22%2C%22vurl%22%3A%224166%22%7D%2C%22partnerParameterName%22%3A%22slimprid%22%7D **URI:** http://trk.slimwareutilities.com/ulc.php?ev=Startup&installId=52F619EC-34A1-4F9B-9871-8DC5C253D44C&browser=chrome&productVersion=2.7.11.0&product=SW2&hasUI=yes&vurl=4166&s2s=NjM2fDcyODEzfFVTfDQ0fDF8fHx8fA%7C%7C%7C636&up=YToxMjp7czo5OiJ1bF9zdHViaWQiO3M6MzY6IjY1MWJiMzFlLTUzOWMtNDI5MC05NjQyLWM3YzQ1ODVkY2EyMiI7czoxMDoidWxfY29icmFuZCI7czozOiJTVzIiO3M6MTE6InVsX2NhbXBhaWduIjtzOjY6InhkbTYzMyI7czo4OiJ1bF9zdWJpZCI7czozOiI2MzYiO3M6NzoiYWRHcm91cCI7czo0OiI0MTY2IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjEyOiJ1c2VyU2VnbWVudHMiO086ODoic3RkQ2xhc3MiOjE6e3M6MTI6IlBob25lU3VwcG9ydCI7Tzo4OiJzdGRDbGFzcyI6Mjp7czoxMzoiU3VwcG9ydFZlbmRvciI7czo4OiJTbGltV2FyZSI7czoxNzoiU3VwcG9ydE51bWJlclR5cGUiO3M6MTA6IkFjdGl2YXRpb24iO319czoxMToiYnJvd3NlclR5cGUiO3M6NDoiRWRnZSI7czoxNDoiYnJvd3NlclZlcnNpb24iO3M6ODoiMTQuMTQzOTMiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czo0OiIxMC4wIjt9&machineId=1C3D66D7-076C-41B9-AC2A-46C332DE0DA0&isRegistered=no&userSegments=O%3A8%3A%22stdClass%22%3A1%3A%7Bs%3A12%3A%22PhoneSupport%22%3BO%3A8%3A%22stdClass%22%3A2%3A%7Bs%3A13%3A%22SupportVendor%22%3Bs%3A8%3A%22SlimWare%22%3Bs%3A17%3A%22SupportNumberType%22%3Bs%3A10%3A%22Activation%22%3B%7D%7D&eventSource=SYSTEM&scanPagePixel=%7B%22parameters%22%3A%7B%22slimprid%22%3A%22%5ESW2%5Exdm633%22%2C%22s2s%22%3A%22NjM2fDcyODEzfFVTfDQ0fDF8fHx8fA%7C%7C%7C636%22%2C%22vurl%22%3A%224166%22%7D%2C%22partnerParameterName%22%3A%22slimprid%22%7D						
www.slimwareutilities.com	80	GET	1.1	DriverUpdate	1	135.025968075
Path: /download_stats/new_install.php?program=DriverUpdate2 **URI:** http://www.slimwareutilities.com/download_stats/new_install.php?program=DriverUpdate2						
trk.slimwareutilities.com	80	GET	1.1	SLIMHTTP/1.1	1	144.9854002
Path: /ulc.php?ev=Startup&installId=52F619EC-34A1-4F9B-9871-8DC5C253D44C&browser=chrome&productVersion=2.7.11.0&product=SW2&hasUI=no&vurl=4166&s2s=NjM2fDcyODEzfFVTfDQ0fDF8fHx8fA%7C%7C%7C636&upl=YToxMjp7czo5OiJ1bF9zdHViaWQiO3M6MzY6IjY1MWJiMzFlLTUzOWMtNDI5MC05NjQyLWM3YzQ1ODVkY2EyMiI7czoxMDoidWxfY29icmFuZCI7czozOiJTVzIiO3M6MTE6InVsX2NhbXBhaWduIjtzOjY6InhkbTYzMyI7czo4OiJ1bF9zdWJpZCI7czozOiI2MzYiO3M6NzoiYWRHcm91cCI7czo0OiI0MTY2IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjEyOiJ1c2VyU2VnbWVudHMiO086ODoic3RkQ2xhc3MiOjE6e3M6MTI6IlBob25lU3VwcG9ydCI7Tzo4OiJzdGRDbGFzcyI6Mjp7czoxMzoiU3VwcG9ydFZlbmRvciI7czo4OiJTbGltV2FyZSI7czoxNzoiU3VwcG9ydE51bWJlclR5cGUiO3M6MTA6IkFjdGl2YXRpb24iO319czoxMToiYnJvd3NlclR5cGUiO3M6NDoiRWRnZSI7czoxNDoiYnJvd3NlclZlcnNpb24iO3M6ODoiMTQuMTQzOTMiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czo0OiIxMC4wIjt9&machineId=1C3D66D7-076C-41B9-AC2A-46C332DE0DA0&isRegistered=no&userSegments=O%3A8%3A%22stdClass%22%3A1%3A%7Bs%3A12%3A%22PhoneSupport%22%3BO%3A8%3A%22stdClass%22%3A2%3A%7Bs%3A13%3A%22SupportVendor%22%3Bs%3A8%3A%22SlimWare%22%3Bs%3A17%3A%22SupportNumberType%22%3Bs%3A10%3A%22Activation%22%3B%7D%7D&eventSource=SYSTEM&scanPagePixel=%7B%22parameters%22%3A%7B%22slimprid%22%3A%22%5ESW2%5Exdm633%22%2C%22s2s%22%3A%22NjM2fDcyODEzfFVTfDQ0fDF8fHx8fA%7C%7C%7C636%22%2C%22vurl%22%3A%224166%22%7D%2C%22partnerParameterName%22%3A%22slimprid%22%7D **URI:** http://trk.slimwareutilities.com/ulc.php?ev=Startup&installId=52F619EC-34A1-4F9B-9871-8DC5C253D44C&browser=chrome&productVersion=2.7.11.0&product=SW2&hasUI=no&vurl=4166&s2s=NjM2fDcyODEzfFVTfDQ0fDF8fHx8fA%7C%7C%7C636&upl=YToxMjp7czo5OiJ1bF9zdHViaWQiO3M6MzY6IjY1MWJiMzFlLTUzOWMtNDI5MC05NjQyLWM3YzQ1ODVkY2EyMiI7czoxMDoidWxfY29icmFuZCI7czozOiJTVzIiO3M6MTE6InVsX2NhbXBhaWduIjtzOjY6InhkbTYzMyI7czo4OiJ1bF9zdWJpZCI7czozOiI2MzYiO3M6NzoiYWRHcm91cCI7czo0OiI0MTY2IjtzOjc6InByb2R1Y3QiO3M6MzoiU1cyIjtzOjEyOiJ1c2VyU2VnbWVudHMiO086ODoic3RkQ2xhc3MiOjE6e3M6MTI6IlBob25lU3VwcG9ydCI7Tzo4OiJzdGRDbGFzcyI6Mjp7czoxMzoiU3VwcG9ydFZlbmRvciI7czo4OiJTbGltV2FyZSI7czoxNzoiU3VwcG9ydE51bWJlclR5cGUiO3M6MTA6IkFjdGl2YXRpb24iO319czoxMToiYnJvd3NlclR5cGUiO3M6NDoiRWRnZSI7czoxNDoiYnJvd3NlclZlcnNpb24iO3M6ODoiMTQuMTQzOTMiO3M6MTU6ImJyb3dzZXJMYW5ndWFnZSI7czo1OiJlbi11cyI7czoxMDoicGxhdGZvcm1PUyI7czo3OiJXaW5kb3dzIjtzOjE3OiJwbGF0Zm9ybU9TVmVyc2lvbiI7czo0OiIxMC4wIjt9&machineId=1C3D66D7-076C-41B9-AC2A-46C332DE0DA0&isRegistered=no&userSegments=O%3A8%3A%22stdClass%22%3A1%3A%7Bs%3A12%3A%22PhoneSupport%22%3BO%3A8%3A%22stdClass%22%3A2%3A%7Bs%3A13%3A%22SupportVendor%22%3Bs%3A8%3A%22SlimWare%22%3Bs%3A17%3A%22SupportNumberType%22%3Bs%3A10%3A%22Activation%22%3B%7D%7D&eventSource=SYSTEM&scanPagePixel=%7B%22parameters%22%3A%7B%22slimprid%22%3A%22%5ESW2%5Exdm633%22%2C%22s2s%22%3A%22NjM2fDcyODEzfFVTfDQ0fDF8fHx8fA%7C%7C%7C636%22%2C%22vurl%22%3A%224166%22%7D%2C%22partnerParameterName%22%3A%22slimprid%22%7D						

DNS QUERIES

Request	Type
www.slimwareutilities.com	A
Answers - slimwareutilities.com (CNAME) - 50.17.223.81 (A)	
stats.slimwareutilities.com	A
Answers - 54.231.40.17 (A) - 52.216.224.226 (A)	
trk.slimwareutilities.com	A
Answers - trk-slimwareutilities-com-ms-270141606.us-east-1.elb.amazonaws.com (CNAME) - 34.231.33.210 (A) - 52.54.9.186 (A) - 54.175.217.102 (A)	
download.driverupdate.net	A
Answers - 13.33.80.36 (A) - 13.33.80.10 (A) - 13.33.80.149 (A) - 13.33.80.116 (A)	
cdn.slimcleaner.com	A
Answers - 13.33.80.117 (A) - 13.33.80.145 (A) - 13.33.80.46 (A) - 13.33.80.96 (A)	
ctldl.windowsupdate.com	A
Answers - audownload.windowsupdate.nsatc.net (CNAME) - cs11.wpc.v0cdn.net (CNAME) - wu.ec.azureedge.net (CNAME) - hlb.apr-52dd2-0.edgecastdns.net (CNAME) - 72.21.81.240 (A) - wu.azureedge.net (CNAME) - wu.wpc.apr-52dd2.edgecastdns.net (CNAME)	
ocsp.verisign.com	A
Answers - ocsp-ds.ws.symantec.com.edgekey.net (CNAME) - e8218.dscb1.akamaiedge.net (CNAME) - 23.35.171.27 (A)	
sf.symcd.com	A
Answers - 23.54.187.27 (A)	
stc.slimwareutilities.com	A
Answers - stc-slimwareutilities-com-ms-1989010110.us-east-1.elb.amazonaws.com (CNAME) - 52.55.74.238 (A) - 52.20.7.33 (A)	

Request	Type
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)	
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)	
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)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
5.97793507576	Sandbox	50.17.223.81	80
7.76453208923	Sandbox	54.231.40.17	80
8.48067808151	Sandbox	34.231.33.210	80
8.63656711578	Sandbox	13.33.80.116	80
12.9094910622	Sandbox	13.33.80.46	80
18.6425011158	Sandbox	72.21.81.240	80
24.0406351089	Sandbox	23.35.171.27	80
29.3270590305	Sandbox	23.54.187.27	80
33.8816361427	Sandbox	54.175.217.102	80
33.9617540836	Sandbox	52.216.224.226	80
45.3612411022	Sandbox	52.20.7.33	80
45.5479290485	Sandbox	13.33.80.46	80
45.5486860275	Sandbox	54.175.217.102	80
57.5836369991	Sandbox	23.54.187.27	80
65.046749115	Sandbox	23.215.131.200	80
83.0204370022	Sandbox	151.101.2.133	80
133.790081024	Sandbox	52.44.174.33	80
134.102061987	Sandbox	34.231.33.210	80
135.025968075	Sandbox	50.17.223.81	80
144.32811904	Sandbox	52.44.174.33	80
144.9854002	Sandbox	34.231.33.210	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.08527112007	Sandbox	192.168.56.255	137
3.09007310867	Sandbox	224.0.0.252	5355
3.09216618538	Sandbox	224.0.0.252	5355
3.14172005653	Sandbox	239.255.255.250	3702
5.65179204941	Sandbox	224.0.0.252	5355
5.8789601326	Sandbox	8.8.4.4	53
5.8793900013	Sandbox	224.0.0.252	5355
6.02601599693	Sandbox	224.0.0.252	5355
7.70508098602	Sandbox	8.8.4.4	53
7.7526640892	Sandbox	224.0.0.252	5355
8.43930411339	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
8.57932806015	Sandbox	8.8.4.4	53
10.285531044	Sandbox	224.0.0.252	5355
12.8456141949	Sandbox	8.8.4.4	53
13.3605771065	Sandbox	224.0.0.252	5355
15.9425301552	Sandbox	224.0.0.252	5355
18.5019440651	Sandbox	8.8.4.4	53
18.8402581215	Sandbox	224.0.0.252	5355
21.40417099	Sandbox	224.0.0.252	5355
23.9544291496	Sandbox	8.8.4.4	53
24.1589691639	Sandbox	224.0.0.252	5355
26.7333021164	Sandbox	224.0.0.252	5355
29.2829961777	Sandbox	8.8.4.4	53
31.205242157	Sandbox	224.0.0.252	5355
33.7673821449	Sandbox	8.8.4.4	53
33.9063110352	Sandbox	8.8.4.4	53
42.2891490459	Sandbox	224.0.0.252	5355
42.5663499832	Sandbox	224.0.0.252	5355
45.2364711761	Sandbox	8.8.4.4	53
51.5474641323	Sandbox	224.0.0.252	5355
54.8289310932	Sandbox	224.0.0.252	5355
57.5320901871	Sandbox	8.8.4.4	53
58.7849330902	Sandbox	224.0.0.252	5355
62.0484189987	Sandbox	224.0.0.252	5355
64.8440711498	Sandbox	8.8.4.4	53
65.240309	Sandbox	224.0.0.252	5355
67.9573609829	Sandbox	224.0.0.252	5355
70.8502640724	Sandbox	224.0.0.252	5355
73.9077250957	Sandbox	224.0.0.252	5355
77.3973550797	Sandbox	224.0.0.252	5355
80.1921219826	Sandbox	224.0.0.252	5355
82.9542181492	Sandbox	8.8.4.4	53
130.067040205	Sandbox	224.0.0.252	5355
133.65993619	Sandbox	8.8.4.4	53
134.044691086	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 9bc1fb955999ab89639a5bf1ed0b98d0 **SHA-1 :** 8d8c00ddd5ebc193ec9265e25a01399f5c687c62 **SHA-256 :** 26c8797aa8d65d0808a4960efd003b02a7a296b(**SHA-512 :** b6115d29e1d933dff2d34de065b396427790528(**Size :** 2.576 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 9d0e43086e5fa928f99bc8db19f762f1 **SHA-1 :** cb7b34169dde3c714bb3c992e059e232aedbfe0a **SHA-256 :** b99f1b4b069a6ae79c8a184598c3d110eab3267! **SHA-512 :** 9989dafb7f72ab923dc66514cf52ad23b468eeac(**Size :** 1.544 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\9A19ADAD9D098E039450ABBEDD5616EB_90968CAB679DC8A66D51322A089E7CBE	**Type :** data **MD5 :** 2d81acc64cf19cb4c66c89241c1685c2 **SHA-1 :** c3cae895f29de20eaea2efa00578bae21da1aedb **SHA-256 :** c96f5927cdede988989ee359ad9147ca8ff006cc0 **SHA-512 :** e7cf66fbdd7d3f95bcc17b5b4acd09b3fc15bd99c **Size :** 1.66 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 08651b6757174456b82cd0fca3167de3 **SHA-1 :** 95b9acceebd057b92fc3da824915ceaca5348fb7 **SHA-256 :** 07d5fa9fb617333b112a9c3929274e255858c570 **SHA-512 :** 9f84b1888afa3729bf54d19d1190d664d5844391 **Size :** 1.544 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 7fa72498912201a83c16c5b6c2a797cd **SHA-1 :** d6de1907c783a1daf07fd297ef0235fbcde170c3 **SHA-256 :** c1e3721bc82fc3b000b753d520c83892c7158d36 **SHA-512 :** 75f094a13f74ce5c24baf453446f7de2956f107eaf **Size :** 2.576 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 :** 9446e8f2056fea3ac1365a809ada04602606242c **SHA-512 :** 75763aa13b43eb96294b0f84e13106611198872(**Size :** 6.509 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Supdates.Db-Journal	**Type :** dBase IV DBT, blocks size 3613630752, next free block index 4177909209 **MD5 :** 84e6140546860f9aaf5d41ee1d64296c **SHA-1 :** 65317aa23e9a1eebfb7c84eb323ac32dad796184 **SHA-256 :** d6b6c64fbd4befb7a113aaeae13c908ddf9fea1eb **SHA-512 :** ae779aab087de428f36ea844925511477841ce46 **Size :** 0.512 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 244a5978dc48ea4e9c99a11703ca9ec0 **SHA-1 :** 2169f659dee405039a0d73ab68ad6e975d512198 **SHA-256 :** 7b9cd8db82a4f73a7f62c7cf2459fc3e979377a98 **SHA-512 :** 45e7119ffa50484d78f7b912359b22ec72ed1e5d **Size :** 5.672 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 61a6713a000dae9f46702a27cf336c7d **SHA-1 :** 9e9d8dbce13533e88a7d87ab6368e5ee476503ec **SHA-256 :** 73e01e7fa76f336d9421a13e1188e5eb67b56ff0 **SHA-512 :** f98b11eec900720e6740e3f0cf81334b7f16e9a93 **Size :** 5.672 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** dfcbf25623e24fc596d4b66b8a9e663b **SHA-1 :** f588168fe1199ce0e12882feb1e01d555db07a89 **SHA-256 :** 890969cd7c1fb31bb29406532a47d5a6536a860 **SHA-512 :** 149b1469897b924ef723b3d2a3be1ab1e76bb0c **Size :** 2.576 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\SWDUMon.Sys **C:\Windows\Sysnative\Drivers\SWDUMon.Sys**	**Type :** PE32+ executable (native) x86-64, for MS Windows **MD5 :** 04cf20310145dec63d5387beaff77d9a **SHA-1 :** 1e0e9f8751402b3484f765e0709209e2a96e9f5c **SHA-256 :** 5017af8c2dfbfe1f9946ff5af229d62d141118ea92 **SHA-512 :** e3c3b4409d31fdbdf9184c58e01845dc8e4664c0 **Size :** 13.92 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Supdates.Db-Journal	**Type :** data **MD5 :** 7b813bce4183bc14a79da745ecb5b065 **SHA-1 :** 1b2eda220343a80e4fa635f89416c9d12d51f09a **SHA-256 :** 0427b10b46a030ebd67bf6b0b3c2c9ffd710a0fa **SHA-512 :** a65be5821e4a34d7a908c50126437f94c084c3ac **Size :** 1.544 Kilobytes.
C:\Users\User\AppData\Local\Temp\Scp78E5.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 :** 5052eb0b14ce2cd373b68933c3422146 **SHA-1 :** 506fcaa45ae95c734d6f23328bdc8dc3dd825930 **SHA-256 :** ce75c102b80380f005e30cbac20b549206612d35 **SHA-512 :** 4099916af86bfe5b58fd0898400bac7acfb60e577 **Size :** 2.576 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Supdates.Db-Journal	**Type :** data **MD5 :** a6af5cc66368752d6d98bcfbd69be81c **SHA-1 :** 37982350f6e4bf015d9a84d109d49855d1005e14 **SHA-256 :** 98ec380b8a1bb72cb15caf0ece78a5f4e15ce2f06 **SHA-512 :** d64783d95262d968842b44656784597d5b1179f **Size :** 1.544 Kilobytes.
C:\Windows\Inf\Setupapi.App.Log	**Type :** ASCII text, with CRLF line terminators **MD5 :** 2acb67e0afbb97b07ee6db6ef586b7d9 **SHA-1 :** eb145d9d0e0a4380e9f953bdf4a9d24e013f997b **SHA-256 :** 6b774b94ed9afbe2c32660c4bf927bea1ff14e3aa **SHA-512 :** dd12543cecceaa098038c26bb133f161cf5367f06 **Size :** 106.206 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Supdates.Db-Journal	**Type :** data **MD5 :** af1ec92ec0ff9ecbee100f490ef658a7 **SHA-1 :** 9d809bee3c04c0be10f732030903124d30ef6d07 **SHA-256 :** 5087902ac13bb4bb867f63b8984943e764e22a0 **SHA-512 :** 58e88c203398a394c07c8d6c70aa14912c45327f **Size :** 1.544 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 75329fe36ff1ff65130c365adb1d9d0f **SHA-1 :** b409c8287ad9ce7ad9f4488785a8a106ad362252 **SHA-256 :** 80dd0ede163a1236e00445ed32d263104bd1d1e **SHA-512 :** 45036d1ad63c0649e391de981690fc543c83847c **Size :** 2.576 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\SWDUMon.Cat	**Type :** data **MD5 :** 0b1da72305373dba342a749ce9a4402e **SHA-1 :** 8db059f27c70193cf9f71cd3f72f5f2db2528ddf **SHA-256 :** 60a36a7d6ad77d392b355950fb6877f804be0a15 **SHA-512 :** ad64ea8e4a01b25b3c0124f7f462f137198550cfa **Size :** 7.584 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 :** 1a53ad4fbec13afcabdf1c3bae0f0387 **SHA-1 :** 90293f7e5ab8a312e6fae18e100988176f621dc4 **SHA-256 :** 40379ff952cb783c5742ec619aa53c92229c5253b **SHA-512 :** d4c7801f4114d2975cd1f42fbabf5ad5d08bb27f6 **Size :** 0.512 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Supdates.Db-Journal	**Type :** data **MD5 :** df32b9a2a1c2383110f9e8d39df57114 **SHA-1 :** 87517c78fc6f0bbccd5dfa6fe72ef717c6ac693e **SHA-256 :** 582f44307ad0043d7ed224e42bbbd292f10c4af8 **SHA-512 :** 49f23756e513f1644b2dd93e35fd515948766c5cb **Size :** 1.544 Kilobytes.
C:\Users\User\AppData\Local\Temp\MSIc9283.LOG	**Type :** Little-endian UTF-16 Unicode text, with very long lines, with CRLF line terminators **MD5 :** 7d6b1e6613dbf024bc2ba7fd726f3935 **SHA-1 :** 5fc84ba9a7ea00e4e85afc36192dfe631eb675e0 **SHA-256 :** 5bed3f235df0bbbd90afabdbc5e23e5332fb29b1 **SHA-512 :** 1bf6e9f1a655b059f2308fe78f5134a454e2b79d1 **Size :** 145.838 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Logs\2018-10-20 12-38-29 0.Log	**Type :** ASCII text, with CRLF line terminators **MD5 :** 36ba0c2cb32ae3a3b03c009bbd209db8 **SHA-1 :** 272f25d6623c7ab30dad737a843827573adcdd2d **SHA-256 :** d523fdfd5763e9c086dc43bb552924ffe3a1a9aaa **SHA-512 :** abbd5e9b91840e5f38fcf2fe820d3811c3b0e190c **Size :** 0.819 Kilobytes.
C:\Users\User\AppData\Local\Temp\Scp78E5.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.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\SIOUT13346281\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 14:15:38 2018, Last Saved Time/Date: Mon Jun 18 14:15:38 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\LocalLow\Microsoft\CryptnetUrlCache\Content\9A19ADAD9D098E039450ABBEDD5616EB_04EB95CBF9CF5CBD7E29D6EC69DB8985	**Type :** data **MD5 :** 0d01fcd2b88ff00566f7d983b3722db0 **SHA-1 :** cc0182f08c939652a85564e0ad4a7eb477587c56 **SHA-256 :** 11300c4e4afafdcabb98a21c8be673468d2d2a65 **SHA-512 :** a8376828bb119577c17138913616a2709868f11f **Size :** 1.66 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\9A19ADAD9D098E039450ABBEDD5616EB_90968CAB679DC8A66D51322A089E7CBE	**Type :** data **MD5 :** 87d717155875ab8b64ecf2eb1374e8e5 **SHA-1 :** 47be024f73991426579d788a0a6d7f84e80e8a6c **SHA-256 :** c646cb8715dd8de8aa9d68c5b7e835643f7deca1 **SHA-512 :** 53ea334a438dd77c0b4525c6b45e56c995b180c3 **Size :** 0.398 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** e77dfcab9689bd5540fb5237301f472e **SHA-1 :** 61d1563b1f5b68eb18afdf29ab5b93c770e5c478 **SHA-256 :** 362dddf3a36563f60a0d0dfbc902d1b81ab095f7 **SHA-512 :** d6fa8750668b735cded37bc9128df8996badf3f8 **Size :** 6.704 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** f451f0e26b6df8886d95eb902de2a3bc **SHA-1 :** 6f767122675ff2f90ca4aaf2893933d215a3ff05 **SHA-256 :** 2030c9ae2e6b7c5fcd2400a1ad2526e422e00890 **SHA-512 :** 9bd3c39c681136a5c61321f0d5dd934e2316293 **Size :** 5.672 Kilobytes.
C:\Users\User\AppData\Local\Temp\SlimCleanerPlus_en-US_x64_Silent.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 075a229499b5ceaa0f439d4a5f01ff08 **SHA-1 :** 91c5827500b047ef80fa23347d02bdc56e0bab22 **SHA-256 :** e9caeed965005ceee2c1e3284af4201b95c8f66d **SHA-512 :** a79c8e39cae531a8f4fb653239bedcdec282309e **Size :** 18697.568 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** c33a8dda895a54386108f5a4ff5cd688 **SHA-1 :** 883265cfc8b45693540e0bdbb70ddc4a95a3d38b **SHA-256 :** ce92a3c0be22ad5329689998e9352c2d71efe431 **SHA-512 :** 4403b7bf4d31a7d1f0945ea8264ea4a8fd4db507 **Size :** 0.342 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** b0612fac2773cea668334f0543c5905e **SHA-1 :** 1ba6f0c8a077bcf372f80de8279b0be75fcdb5e8 **SHA-256 :** 5509d702bf433dfcbc7d4b8fd493b79f427e35d6 **SHA-512 :** 4ad3b94d28243c6bba3b76018f9f8975c9071b4a **Size :** 5.672 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** c89e14098b88be2e827057d45a722042 **SHA-1 :** 820a3fa3b74a79353c28c68601ffebe19acf0418 **SHA-256 :** c6eac91c0a6f056581b8daa9e38b0c59d72b03c6 **SHA-512 :** f29d4b0306945191f5ee3f852af2745207321f5c5 **Size :** 5.672 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Logs\2018-10-20 12-38-38 0.Log	**Type :** ASCII text, with CRLF line terminators **MD5 :** dd23995a0d7aa675e0088f3a84bc69cd **SHA-1 :** 94a9be1ebe68292529470b0f4cbeb9e62522285c **SHA-256 :** 8fd002fab5b993486e0567449203e7d4a2cbde4f **SHA-512 :** e0cd68602842db7d9b4230dbc6bb4e99a4577e9 **Size :** 0.133 Kilobytes.
C:\Users\User\AppData\Local\Temp\MSIbda57.LOG	**Type :** Little-endian UTF-16 Unicode text, with very long lines, with CRLF line terminators **MD5 :** 6fe0e865e5afe7099d404b46221a6ebe **SHA-1 :** 9e67eb289ce4039ffe7ec27b581677da556af678 **SHA-256 :** 21f8aa687ddefdb15cdc6e801e59bcbd2b0c4f2d **SHA-512 :** 73c76ba683387980d35e559fb7a500159de6b57 **Size :** 305.596 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\SWDUMon.Inf	**Type :** ASCII text, with CRLF line terminators **MD5 :** b65ddb94d2d123934de74e627ccc663c **SHA-1 :** e4a6427eed2e35df1f77476e65af1caa4b8a1a37 **SHA-256 :** 26f246efad9dbde96fa3ca39352e986deb31bf35(**SHA-512 :** 408139262086c4c9e8b5b255017c101ecc6199f8 **Size :** 1.639 Kilobytes.
C:\Users\User\AppData\Local\Temp\Swu683A.Tmp	**Type :** bzip2 compressed data, block size = 900k **MD5 :** aaca9bff28318371a621f922da4c2af3 **SHA-1 :** 164c688c60c4c07810955bb30313d0ea16f5e07a **SHA-256 :** 34b002f8f0b461a3e6eaeb0fc821914e842939d7 **SHA-512 :** ebc0b076d81c4ece5b7f8cd7fdd0584b04dd1e79 **Size :** 3681.334 Kilobytes.
C:\Users\User\AppData\Local\Temp\Swu683A.Tmp.Msi **C:\Users\Public\Documents\Downloaded Installers\{055C7DA5-A1F5-41FB-932C-82474ED3487A}\Setup.Msi**	**Type :** Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.3, Code page: 1252, Title: Installation Database, Subject: Looks for updates for your computer's software and drivers to improve performance., Author: Slimware Utilities Holdings, Inc., Keywords: update, software, drivers, Comments: This installer database contains the logic and data required to install DriverUpdate., Template: Intel;1033, Revision Number: {8BA6BC7B-FA09-46C3-8633-322698E0999B}, Create Time/Date: Wed Jul 19 19:02:22 2017, Last Saved Time/Date: Wed Jul 19 19:02:22 2017, Number of Pages: 200, Number of Words: 2, Name of Creating Application: Windows Installer XML Toolset (3.9.1208.0), Security: 2 **MD5 :** 2dfb22e30d15b09ffd03997ca388ad19 **SHA-1 :** fb66ebb7cbdb3644585c3261800f951c492475f2 **SHA-256 :** e532c509b45f15c469c0186dd26b68f1e0502476 **SHA-512 :** 0444bd12ab254931ff86ed948b3e0cfa8da88c1fe **Size :** 30523.392 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7D266D9E1E69FA1EEFB9699B009B34C8_0A9BFDD75B598C2110CBF610C078E6E6	**Type :** data **MD5 :** 3ae470dfab885b9aa65b58285e099672 **SHA-1 :** 2bcd121ce126a40b95a2cba39fc094287109a42c **SHA-256 :** d0fbb46d62100b639687f7a7d52ea6b8f32049d4 **SHA-512 :** 411773244872ebb4f90aa586f2aab19203844128 **Size :** 0.404 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Supdates.Db	**Type :** SQLite 3.x database **MD5 :** 502c79a63a307fe999ef82f77a1ceb97 **SHA-1 :** a94bde1e7e3a469e542041ed05c8a0a9ffdf7f52 **SHA-256 :** 638926cc308abe0d3187f03c815acec0c502e9fb1 **SHA-512 :** 7da85d9a97f11ef9130928bc2b34d95ac09990db **Size :** 8.192 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Supdates.Db-Journal	**Type :** data **MD5 :** 849551ab03e1d2fed52d3f3d57d1b9c1 **SHA-1 :** 56e2144502c156f5389795b11d3991ae5c85dd6a **SHA-256 :** 4a345d4743b24b40650f5029f284dec0ba24c3e2 **SHA-512 :** 7e67b258b06ccae734c94c581245bde2998e0e02 **Size :** 1.544 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7D266D9E1E69FA1EEFB9699B009B34C8_0A9BFDD75B598C2110CBF610C078E6E6	**Type :** data **MD5 :** 34da152486c1039b52458c90abc450c9 **SHA-1 :** e56105ba53cfc59c8b4c7f004d47a5a7a7d0b4c0 **SHA-256 :** 37f50129077fbccc361cb19c78e7a1bdae6e083a8 **SHA-512 :** 004179b7e0e1a3725da465fae565bab786c7f344 **Size :** 1.754 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 422256b3d1d6fb5e5a025eef6e9a7908 **SHA-1 :** f2e3533924909d8b30068884b325ac985c33d6dc **SHA-256 :** 40327d96bbd74dcf69a626888fca645ebe5370b8 **SHA-512 :** aef60d98b099d8a7ea2b8c53830eedf2151081bb **Size :** 5.672 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** a991dd4cafe431f02bacb7aba284dd38 **SHA-1 :** ccf7d99428ad43f22ade5af74f4629f469e41dc8 **SHA-256 :** dd2c85a33abbc7a2684483ad43d2362e2429f52a **SHA-512 :** 40325807f57d8f1c322c29518ed0afddd7f66bf39 **Size :** 1.544 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** 8852f4c29c34c6dd656af4a27108bcec **SHA-1 :** 535faad0e1bd8558afa3e80dfa717a8a6d4b9214 **SHA-256 :** 04421930db4dda6bfe5f0bc3e59093a7c207edb2 **SHA-512 :** e08d06c41f0441be2e5be4876215b0547339927 **Size :** 2.576 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db	**Type :** SQLite 3.x database **MD5 :** d12b49aace6934d24c6f3e7faa49b971 **SHA-1 :** bafc0012aa087c2ce1d53a33f2447378bee5c82b **SHA-256 :** 535a51a54b02e3da1c68ec58e5d8dfe5d2bc278f **SHA-512 :** 3e582e9da0e28409ebab2b1fdf673d9ed35e2217 **Size :** 9.216 Kilobytes.
C:\Users\User\AppData\Local\SlimWare Utilities Inc\DriverUpdate\Settings.Db-Journal	**Type :** data **MD5 :** fe100d54db9308a69b0b7bc00777fc5a **SHA-1 :** 2639e33174a97f9e14d493d334f456cde35d1f12 **SHA-256 :** a5e5a196bb9cd46c10ecb25139f902a388830b9e **SHA-512 :** 0bf3d96d8056c8b0bf92a157fa762cb710fed68d8 **Size :** 5.672 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\9A19ADAD9D098E039450ABBEDD5616EB_04EB95CBF9CF5CBD7E29D6EC69DB8985	**Type :** data **MD5 :** 588e45323fe22aeb50379fae8dd08701 **SHA-1 :** 3c2eccda3262ced3779a4783528bce88ab3a11f6 **SHA-256 :** b61c5e5e94ea344b542e9a9b61cc624025419af4 **SHA-512 :** 5509ecf18022b210d99dd3af74db77f147c4aa03 **Size :** 0.394 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	None
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	411c2a9901a0c1fe105dfa5e486cdc420bb3f145
MD5:	58adb00645d0cb56306a81935e854733
First Seen Date:	2018-10-19 05:09:33.893505 (4 months ago)
Number Of Clients Seen:	3
Last Analysis Date:	2018-10-19 05:09:33.893505 (4 months ago)
Human Expert Analysis Date:	2018-10-22 14:44:13.661220 (4 months ago)
Human Expert Analysis Result:	PUA

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[{u'Path': u'E:\\BuildAgent\\work\\cdc3d0ebfd4f8694\\bin\\Release\\LittleInstaller.pdb\x00', u'GUID': u'{c79b1cf9-16a5-41ab-8d2e-42f6f85d8e8a}', u'timestamp': u'2016-07-30 16:10:51'}]
Number Of Sections	5
Trid	[[67.4, u'Win32 Executable MS Visual C++ (generic)'], [14.2, u'Win32 Dynamic Link Library (generic)'], [9.7, u'Win32 Executable (generic)'], [4.3, u'Generic Win/DOS Executable'], [4.3, u'DOS Executable Generic']]
Compilation Time Stamp	0x579CD18B [Sat Jul 30 16:10:51 2016 UTC]
LegalCopyright	Copyright 2011-2016 Slimware Utilities Holdings, Inc.
InternalName	LittleInstaller
FileVersion	2.7.1
CompanyName	Slimware Utilities Holdings, Inc.
ProductName	DriverUpdate
ProductVersion	2.7.1
FileDescription	DriverUpdate Setup Wizard
OriginalFilename	DriverUpdate-setup.exe
Translation	0x0409 0x04b0
Entry Point	0x4376bb (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	991608
Ssdeep	12288:PRXk1egQfxyGaaI1PDUO76+XKTYvnqFo78CrCU9YPN:ZGAO9DUO3kYvb8COnPN
Sha256	f756bc9033641a800b2641cd1e9c3fd31b84b22ce63345d23eb0bbef687c21fc
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/4/1/1/c/411c2a9901a0c1fe105dfa5e486cdc420bb3f145', u'EXE:OriginalFileName': u'DriverUpdate-setup.exe', u'EXE:ProductName': u'DriverUpdate', u'EXE:InternalName': u'LittleInstaller', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:10:19 05:09:08+00:00', u'EXE:InitializedDataSize': 634880, u'File:FileModifyDate': u'2018:10:19 05:09:08+00:00', u'EXE:FileVersionNumber': u'2.7.1.0', u'EXE:FileVersion': u'2.7.1', u'File:FileSize': u'968 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Windows NT 32-bit', u'EXE:ProductVersion': u'2.7.1', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'Slimware Utilities Holdings, Inc.', u'File:FileName': u'411c2a9901a0c1fe105dfa5e486cdc420bb3f145', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2016:07:30 16:10:51+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Copyright 2011-2016 Slimware Utilities Holdings, Inc.', u'EXE:LinkerVersion': 8.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/4/1/1/c', u'EXE:FileDescription': u'DriverUpdate Setup Wizard', u'EXE:EntryPoint': u'0x376bb', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 348160, u'File:FileInodeChangeDate': u'2018:10:19 05:09:08+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'2.7.1.0'}]
Mime Type	application/x-dosexec
Imphash	e85cfcade1b885be4607ae52008eba57

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x54f0c	0x55000	6.63792664922	dac79876157ee0f0ba978a563faa3e33
.rdata	0x56000	0x17d1a	0x18000	4.6823090837	d5e031e5f0dc45391315435e5b8272ae
.data	0x6e000	0x7ebc	0x4000	4.71301588376	d947a72ae9353e2f3d37c83d487eb597
.rsrc	0x76000	0x6df6e	0x6e000	5.8326538553	ed2c04813bbb97aef85b84400ea8a1e4
.reloc	0xe4000	0xcb70	0xd000	4.09321703652	6c86e5ffff6bc51a3f5e33e2c950d936

PE Imports

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

- GlobalFlags
- WritePrivateProfileStringW
- 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
- GlobalAlloc
- GlobalFree
- lstrlenA
- FindResourceExW
- GetFileSize
- CreateFileMappingW
- MapViewOfFileEx
- UnmapViewOfFile
- GetFileSizeEx
- LoadLibraryA
- InterlockedExchange
- FreeLibrary
- LocalAlloc
- GetUserDefaultUILanguage
- WideCharToMultiByte
- ExpandEnvironmentStringsW
- InterlockedDecrement
- InterlockedIncrement
- EnterCriticalSection
- DeleteCriticalSection
- LeaveCriticalSection
- InitializeCriticalSection
- MoveFileExW
- GetSystemDirectoryW
- GetTempPathW
- SetDllDirectoryW
- OutputDebugStringW
- RaiseException
- ReadFile
- SetFilePointer
- FlushFileBuffers
- GetCurrentProcess
- GetCurrentProcessId
- GetCurrentThreadId
- CreateFileW
- GetTempFileNameW

    - VerSetConditionMask
    - VerifyVersionInfoW
    - GetExitCodeProcess
    - DeleteFileW
    - MoveFileW
    - CopyFileW
    - CreateDirectoryW
    - MultiByteToWideChar
    - MulDiv
    - CloseHandle
    - CreateProcessW
    - OpenEventW
    - GetTickCount
    - lstrlenW
    - WaitForSingleObject
    - Sleep
    - GetVersionExW
    - FileTimeToLocalFileTime
    - FileTimeToSystemTime
    - GetUserDefaultLangID
    - GetModuleFileNameW
    - GetProcAddress
    - LoadLibraryW
    - SetLastError
    - GetModuleHandleW
    - GetLastError
    - FormatMessageW
    - FindResourceW
    - LoadResource
    - LockResource
    - SizeofResource
    - GetCommandLineA
    - LocalFree
- USER32.dll
    - DestroyMenu
    - GetMessageW
    - TranslateMessage
    - ValidateRect
    - CharUpperW
    - EndPaint
    - BeginPaint
    - RegisterWindowMessageW
    - SendDlgItemMessageA
    - WinHelpW
    - GetCapture
    - SetWindowsHookExW
    - CallNextHookEx
    - GetClassLongW
    - SetPropW
    - GetPropW
    - RemovePropW
    - GetLastActivePopup
    - DispatchMessageW
    - GetTopWindow
    - UnhookWindowsHookEx
    - GetMessageTime
    - GetMessagePos
    - PeekMessageW
    - MapWindowPoints
    - GetKeyState
    - UpdateWindow
    - GetMenu
    - GetSubMenu
    - GetMenuItemID
    - GetMenuItemCount
    - CreateWindowExW
    - GetClassInfoExW
    - GetClassInfoW
    - RegisterClassW
    - RegisterClipboardFormatW
    - CallWindowProcW
    - SystemParametersInfoA
    - IsIconic
    - GetWindowPlacement
    - GetWindowTextLengthW

- GetWindowTextW
- SetFocus
- MoveWindow
- IsDialogMessageW
- IsDlgButtonChecked
- SetDlgItemTextW
- SendDlgItemMessageW
- CheckDlgButton
- GetDesktopWindow
- GetActiveWindow
- SetActiveWindow
- GetSystemMetrics
- CreateDialogIndirectParamW
- DestroyWindow
- GetDlgItem
- IsWindowEnabled
- GetNextDlgTabItem
- EndDialog
- SetMenuItemBitmaps
- GetMenuCheckMarkDimensions
- LoadBitmapW
- EnableWindow
- SendMessageW
- UnregisterClassA
- GetWindowRect
- RedrawWindow
- GetFocus
- ModifyMenuW
- GetMenuState
- CheckMenuItem
- ShowWindow
- EnumThreadWindows
- WaitForInputIdle
- GetDC
- ClientToScreen
- ScreenToClient
- ReleaseCapture
- SetCapture
- KillTimer
- SetTimer
- InvalidateRect
- ReleaseDC
- SetCursor
- SetRectEmpty
- PtInRect
- TrackMouseEvent
- LoadCursorW
- GetSysColorBrush
- SetWindowTextW
- UnregisterClassW
- EnumChildWindows
- GetClassNameW
- DefWindowProcW
- CopyRect
- IsRectEmpty
- GetSysColor
- CloseWindow
- GetWindow
- PostThreadMessageW
- PostQuitMessage
- FindWindowW
- SetWindowLongW
- GetWindowLongW
- LoadIconW
- GetSystemMenu
- AppendMenuW
- GetForegroundWindow
- PostMessageW
- TabbedTextOutW
- DrawTextW
- DrawTextExW
- GrayStringW
- OffsetRect
- TranslateAcceleratorW
- GetParent

    - DestroyAcceleratorTable
    - IsWindow
    - GetCursorPos
    - MapDialogRect
    - MessageBeep
    - SetRect
    - CreateAcceleratorTableW
    - AdjustWindowRectEx
    - EnableMenuItem
    - SetWindowPos
    - GetWindowThreadProcessId
    - MessageBoxW
    - GetDlgCtrlID
    - FillRect
    - GetClientRect
    - IsWindowVisible
    - SetForegroundWindow
- GDI32.dll
    - DeleteDC
    - GetStockObject
    - DPtoLP
    - ScaleWindowExtEx
    - SetWindowExtEx
    - ScaleViewportExtEx
    - SetViewportExtEx
    - OffsetViewportOrgEx
    - SetViewportOrgEx
    - SelectObject
    - CreateDIBSection
    - MoveToEx
    - LineTo
    - SetMapMode
    - SetBkMode
    - RestoreDC
    - SaveDC
    - SetBkColor
    - SetTextColor
    - GetClipBox
    - CreateBitmap
    - SelectClipRgn
    - GetTextExtentExPointW
    - CreateCompatibleBitmap
    - BitBlt
    - SetBrushOrgEx
    - CreateCompatibleDC
    - CreatePatternBrush
    - GetDeviceCaps
    - GetTextMetricsW
    - Rectangle
    - CreatePen
    - CreateSolidBrush
    - RectVisible
    - PtVisible
    - Escape
    - ExtTextOutW
    - TextOutW
    - CreateFontIndirectW
    - GetObjectW
    - GetTextExtentPoint32W
    - DeleteObject
- COMDLG32.dll
    - GetFileTitleW
- WINSPOOL.DRV
    - DocumentPropertiesW
    - OpenPrinterW
    - ClosePrinter
- ADVAPI32.dll
    - RegEnumKeyExW
    - RegQueryValueW
    - RegEnumKeyW
    - RegDeleteKeyW
    - RegOpenKeyW
    - RegDeleteValueW
    - RegEnumValueW
    - RegCloseKey

- RegQueryInfoKeyW
- RegSetValueExW
- RegCreateKeyExW
- RegQueryValueExW
- RegOpenKeyExW

- SHELL32.dll
  - ShellExecuteW
  - SHGetFolderPathW
  - CommandLineToArgvW
  - Shell_NotifyIconW
- COMCTL32.dll
  - InitCommonControlsEx
- SHLWAPI.dll
  - UrlEscapeW
  - PathFileExistsW
  - PathAppendW
  - SHCreateStreamOnFileEx
  - AssocQueryStringW
  - PathStripToRootW
  - PathIsUNCW
  - PathFindFileNameW
  - PathFindExtensionW
  - UrlEscapeA
- ole32.dll
  - OleIsCurrentClipboard
  - CoCreateInstance
  - CreateStreamOnHGlobal
  - CoCreateGuid
  - StringFromGUID2
  - CoInitializeEx
  - CoUninitialize
  - CoInitialize
  - OleFlushClipboard
  - CoRegisterMessageFilter
  - CoFreeUnusedLibraries
  - OleUninitialize
  - OleInitialize
  - CoRevokeClassObject
- OLEAUT32.dll
  - SysFreeString
  - SysAllocStringByteLen
  - SysStringLen
  - SysAllocString
  - VariantClear
  - VariantInit
  - SysAllocStringLen
  - VariantChangeType
  - LoadRegTypeLib
  - LoadTypeLib
- WS2_32.dll
  - WSAStartup

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 488192, u'sha256': u'fbeb3be87e80cb8e1d2af3d8140796c1bb80c6c7056f60897088ff9e355c3867', u'type': u'data', u'size': 308}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 488500, u'sha256': u'f64ccc0582bc7c66af8b40049e485e8e241335261ec95ace909293ba50b2e4a3', u'type': u'data', u'size': 180}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 488680, u'sha256': u'e7c0005285d1ab59732d5f99f77a9bdd6342b01cf44437ebd7a07611a227e272', u'type': u'data', u'size': 184}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 488864, u'sha256': u'abdf36bde89a26349f5741c17c235dacea88d441d8662ba16a598dc50c3c4864', u'type': u'data', u'size': 324}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 489188, u'sha256': u'ca8fc96218d0a7e691dd7b95da05a27246439822d09b829af240523b28fd5bb3', u'type': u'data', u'size': 744}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 489932, 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': 490228, u'sha256': u'3bbacbad1458254c59ad7d0fd9bea998d46b70b8f8dcfc56aad561a293ffdae3', u'type': u'data', u'size': 2216}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 492444, 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': 493828, u'sha256': u'6e4c3f9044eaf9d157ec8e50bc8a5cd9069b6078058094a4b4a4ab8e6e1ffac1', u'type': u'data', u'size': 68}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 493896, u'sha256': u'300f275bbb1008b2a4367954d64a08db87c680c7bdd0c03615c3a37cfc61a0a9', u'type': u'data', u'size': 366}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 494264, u'sha256': u'4f74a949fe2c9358a546f41a9c598fbe326b432ff17dfbacf2842ac6e7d1787a', u'type': u'data', u'size': 332}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 494596, u'sha256': u'b89eec935455ed0f590248a8446072a56ccc12ab66583b2e54719ec5cf4e2bc1', u'type': u'data', u'size': 362}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 494960, u'sha256': u'62baabd903384fbf221e1149d05900356bd2286c2567e2ce231ee7d168692afe', u'type': u'data', u'size': 526}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 495488, u'sha256': u'e33eb3d08a57cf5dd3710ff2252141f2723984ab13fbebddd2db86f2747ba929', u'type': u'data', u'size': 320}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 495808, u'sha256': u'3b442c077a3c0edd83101d47295701259db768024978619fce3b978e4ccdebdc', u'type': u'data', u'size': 462}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 496272, u'sha256': u'd740b552c6f5879f3193780de45a419aea68ed0e24f1ae2857115f661adc3052', u'type': u'data', u'size': 376}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 496648, u'sha256': u'e16f477b8e47cb4ad9028fb34bb451bdb85c6a8b5bd7f8b18a8088564983e43c', u'type': u'data', u'size': 534}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 497184, u'sha256': u'0da23009e825ebab541af8804f12bf6d64497bd2efb4635a6b8b97ebbb9c84b0', u'type': u'data', u'size': 518}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 497704, u'sha256': u'4cf716efaf68e0cb2ec45ec55d291050b5712b05653cae68edbb999f803d2a98', u'type': u'data', u'size': 52}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 497756, 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': 497976, 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': 498188, 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': 498392, 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': 498564, 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': 498660, u'sha256': u'4803a1975883eb60af94b51e9532e228976461273c7371f3cd133aa4e785819b', u'type': u'data', u'size': 98}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 498760, u'sha256': u'f39b611bd7fd6cf6911947fec504ddde1603149502b794c3f8bb28aa4c088c5f', u'type': u'data', u'size': 120}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 498880, u'sha256': u'ba847dbbcbb4d05fcf8c5c6ca8dbe2e8f1bef3c8ba5bd1862fe1644b2dd73156', u'type': u'data', u'size': 128}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 499008, u'sha256': u'81f3a5cb443e8ad28345f14d4f2ff55aae85e56f3058489e75172ca1164e131d', u'type': u'data', u'size': 82}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 499092, u'sha256': u'258d51f0e31fb7e76662e90b0b6f7276eea18dd7be38bb2f37a883617db56c7a', u'type': u'data', u'size': 68}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 499160, u'sha256': u'08c792e3e0c8c773892a51fc5f1acfabd6bf5556e5e05f33c728e8bec4577610', u'type': u'data', u'size': 258}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 499420, u'sha256': u'da54b5e20f2459b9a25d8b22005d66a8a24dcfdbf5fca99893d5d08515d25586', u'type': u'data', u'size': 314}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 499736, u'sha256': u'fc0ac66e26e5951aa62080e9f15920e54c6aded25923c43f401b69f232a940a6', u'type': u'data', u'size': 340}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 500076, u'sha256': u'897f48ffd80577b462e07038911df69b1607a270b0d83a024c0b7a78361d6aee', u'type': u'data', u'size': 228}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 500304, u'sha256': u'f5f2d753d1a3986f3ce3a955d2b2a1d5af05c5dc69e3a6567f8b75541f0f0db0', u'type': u'data', u'size': 174}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 500480, u'sha256': u'40c1b95e6f501edd0ebff2a2736f38e94f9930b76bfe0a28fed3dd62b1ab47c8', u'type': u'data', u'size': 594}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 501076, u'sha256': u'1056298d4517e7cedfe80bac785d9a4e0fc7b4df0bd1847bf1727a3c259aa2b8', u'type': u'data', u'size': 480}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 501556, u'sha256': u'06025e6f9616ddd627cdca09aac5653e9c890e03c8408f8d4db58a8883c9f19a', u'type': u'data', u'size': 516}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 502072, u'sha256': u'1e5598008e22ef78ff73e17947e5980ffbfbbe8f7d5dd3cf2d8e34e28f175eeb', u'type': u'data', u'size': 380}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 502452, u'sha256': u'309f434d357a58c314d921e23f3411e90628698a9375dfe689281617ff688267', u'type': u'data', u'size': 228}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 502680, u'sha256': u'855d77f3f6ad12a99586b3f021cb2921abaa0504d20855b8c43b314075b26705', u'type': u'data', u'size': 922}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 503604, u'sha256': u'd8f42d3f98d8914f22f4c4d5191487b72903dd1e0905e3bf0986e3b794c29762', u'type': u'data', u'size': 912}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 504516, u'sha256': u'4397ec8a8f18cf20dd80aa59705298089efa88a444cde61ddaaac9fee0e5ea4a', u'type': u'data', u'size': 938}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 505456, u'sha256':

u'1bd8125d5560f1f89cbbf579f9e6e217a0b9499484a3a7f41e6f5c464301ef60', u'type': u'data', u'size': 718}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 506176, u'sha256': u'c5029792d1423ed28055deeda7745563f4f78dcdaa0dbd6b610af7631a433acc', u'type': u'data', u'size': 554}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 506732, u'sha256': u'84050bef84e46fe781f9c5ac7cb30985aef90b23beb97bc425a6fae49cf3cb6a', u'type': u'data', u'size': 290}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 507024, u'sha256': u'ad279e11c370d3e636cf8167bef1a9ea82282bccd80431a100c86d314297d25c', u'type': u'data', u'size': 284}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 507308, u'sha256': u'8d88449cff57219d23f311779473047b16e7efe62f8077e5f053b40931358c0b', u'type': u'data', u'size': 286}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 507596, u'sha256': u'90473bb9384f3f39541eabad15e612fe7c8cd555cbca23fbb06d05ac90aa29a3', u'type': u'data', u'size': 296}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 507892, u'sha256': u'814bebef4ed9fd87c501e2d52feef223193d9a9859a9d0e9a9beca3b69ef7012', u'type': u'data', u'size': 212}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 508104, u'sha256': u'0947cde4cd80ac726e4d7d5d5d966bf16ea1dba641df74265d529724d369d33f', u'type': u'data', u'size': 378}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 508484, u'sha256': u'b69faeb1cc99f8532806c8bf35d553b6ca8293fe32bbd7bd1e2cdfa3d19096ed', u'type': u'data', u'size': 360}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 508844, u'sha256': u'a246ce2c4837b1fbe3d54ed158ffd8fe727105418327bd1f8029263365005412', u'type': u'data', u'size': 344}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 509188, u'sha256': u'fb8e67ea0b8787e4ed24ca15731be79548d684699746bc53a8d3e228f4e71de1', u'type': u'data', u'size': 280}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 509468, u'sha256': u'a7e3c29df3af8134eb884624ec3636b227f5b922d703c3129221986366a749e1', u'type': u'data', u'size': 172}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 509640, u'sha256': u'2ad80490bfbd67e316b34a78c166dfbc8ddbbbac2ac5d3232692fc77dfa32de1', u'type': u'data', u'size': 438}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 510080, u'sha256': u'2cfe0e6e9d5cd1695f2f1028e9936286288f0408d246457ce99509303c1f908f', u'type': u'data', u'size': 426}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 510508, u'sha256': u'fcadde9f221c77e92a26007a43313154e345e09d952ebf6adfa84d2341cc8fa7', u'type': u'data', u'size': 426}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 510936, u'sha256': u'409664bc384377038c8e17156195a88f6819c0273530d451a3edbc0ebe4b9342', u'type': u'data', u'size': 396}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 511332, u'sha256': u'0d10bf879173f9136af0bd077627063c43b2e5609b7bfba7f158544f4429e2e6', u'type': u'data', u'size': 300}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 511632, u'sha256': u'd7e5ec62539ece10aaf1e6edd0518577a5c47cd7b52a7bb62786f5cef00c9c53', u'type': u'data', u'size': 2510}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 514144, u'sha256': u'a6321dcf9148bfcf2d662f75bd02bb2635295f9ba77497dc73f624c13b60de96', u'type': u'data', u'size': 2736}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 516880, u'sha256': u'9c8e58b0377a3119f584fad973251238ce11076805af5039cadbf4640fe1ee0f', u'type': u'data', u'size': 2762}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 519644, u'sha256': u'ab464667e0e22d481aace9368936ac51945356f5f5fb93486c2eed7543dad4db', u'type': u'data', u'size': 2364}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 522008, u'sha256': u'4dc87da676ffc36c51be8e7320341562fc8f888dc30598365d675617d45bcc60', u'type': u'data', u'size': 1620}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 523628, u'sha256': u'a0c2f4fc5a466fda1a6c879e38e6a02c2679a166a855dff600d72cbb12353ef9', u'type': u'data', u'size': 1408}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 525036, u'sha256': u'a8efa60ba5b443fd8048fdd281285d54924802500ab1235a2c5b10a99034c920', u'type': u'data', u'size': 1422}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 526460, u'sha256': u'fe96257d65fa702aff1e703afd9dfe859b97d195898406ae4351ac4f27f1c7b4', u'type': u'data', u'size': 1488}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 527948, u'sha256': u'7ba9fe63361f241a3cf8caf3698f1fd903b3e937b325c8c995c3d93b4affbc9d', u'type': u'data', u'size': 2592}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 530540, u'sha256': u'e275a4adb04f89511ca5ff00b11cfa6148884382c2def8d93956ff4fb3175ee9', u'type': u'data', u'size': 940}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 531480, u'sha256': u'93f45374d169f3144568a8fc503e933842df0e4c60df1cf16aa8274ed1f29d2a', u'type': u'data', u'size': 336}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 531816, u'sha256': u'b29d7f3a4e66d5cc11d25538fccbdbea47f3bcddd5f5617d1efe097f62343e4c', u'type': u'data', u'size': 286}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 532104, u'sha256': u'4f6e434070d9e68aaccf5c49ca2d8ccc2a0d4669f280f9b307a82896b7226ad6', u'type': u'data', u'size': 326}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 532432, u'sha256': u'be18d8c081be944d61d27a48dcee6b9ec93070999d93ef1298f945919bd06560', u'type': u'data', u'size': 270}
{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 532704, u'sha256': u'1517597eae294617a5ce7b3ae21708f652659c4aefb70b494f7dde7e00236592', u'type': u'data', u'size': 194}
{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 532900, u'sha256': u'54e8194c123cb9c249a2e2f4a00a9f688fe77107b3729389a60f7f75e6fb9b45', u'type': u'data', u'size': 1852}
{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 534752, u'sha256': u'245733eceb7bf3399e2a873c74f50df0c9f1433a181cbc788fc29cf1b1606c0b', u'type': u'data', u'size': 1872}
{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 536624, u'sha256': u'2cf55e32d9d900a15a8d3d49c4d19bdc4367f574222ec627ee95737206fdb879', u'type': u'data', u'size': 1926}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 538552, u'sha256': u'bf19f78b7282e1497e7fe7d9abf281f34590eb70dc649c3dcd1c8c810b0a1864', u'type': u'data', u'size': 1432}

{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 539984, u'sha256': u'cc387194724963f52f9babdc60c5c183a6545b0edfc5d32296814197be797b64', u'type': u'data', u'size': 776}

{u'lang': u'LANG_GERMAN', u'name': u'RT_STRING', u'offset': 540760, u'sha256': u'1d076b95d42d95ca2b76268a2e4f105b47b2d421a7cebf64408a12db2f5617a7', u'type': u'data', u'size': 2632}

{u'lang': u'LANG_SPANISH', u'name': u'RT_STRING', u'offset': 543392, u'sha256': u'f128c4d2b371ee4f5af1f2cedc3b3cdda9f4dcc66d08a4199c92a71c6dd0d3b9', u'type': u'data', u'size': 2524}

{u'lang': u'LANG_FRENCH', u'name': u'RT_STRING', u'offset': 545916, u'sha256': u'95e9b90f848a44ed72d60fb3d6cfe6fb56392fb19419a6ec9cc9ece57fcded51', u'type': u'data', u'size': 2698}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 548616, u'sha256': u'2c3e28b5fbc013baa2ac4ed8d1982e20c1b24af439eaab4a619cc3e9ec203eca', u'type': u'data', u'size': 2012}

{u'lang': u'LANG_JAPANESE', u'name': u'RT_STRING', u'offset': 550628, u'sha256': u'f2b8e8d9090ec83112a05b0dea5ee89145db19677acb90d0a5f8b87ed1f7d47c', u'type': u'data', u'size': 1268}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 551896, u'sha256': u'177584c46c7d734f33223e4c585ef9c97ca33a24e49c76b2f20f16964d531920', u'type': u'data', u'size': 56}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 551952, u'sha256': u'291b9c98b2aff4e003dcc57cf5a0a87eff44e0f7803a27282819d0ac6c3a93aa', u'type': u'data', u'size': 62}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 552016, u'sha256': u'66f1747ba4c17f6fca44818ed98445f01645651c120e72f558245e2df6949d35', u'type': u'data', u'size': 402}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 552420, u'sha256': u'0facb5a0cb3ce6df000a594ad8d6428040190be9aaa982716e0587eab374cac9', u'type': u'data', u'size': 906}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 553328, u'sha256': u'c054645d86387fd491743027e6c2284d6a7262f6aced9321cbc1465cef2b6b1f', u'type': u'data', u'size': 794}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 554124, u'sha256': u'c1bc5318a82ea1a1809618040026851947f6aa5171d904a9e60966f4551ca1a3', u'type': u'data', u'size': 732}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 554856, u'sha256': u'1b8660b0c53b94f3e029de58e56d08c8097a080244e9dc65d4155a9b603820d8', u'type': u'data', u'size': 172}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 555028, u'sha256': u'36db380991291cac5c99e42332efda20210f63985544d95e8fa6ef85bf2bdf8e', u'type': u'data', u'size': 1220}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 556248, u'sha256': u'7f51554313c6765ba649783a942064cdfe6f5a70248a6f56840f71969f87ced0', u'type': u'data', u'size': 612}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 556860, u'sha256': u'1f1b61a7f04edc3691a6c9350132b09929d5bfa1c900f6ff500e55c5ebc63212', u'type': u'data', u'size': 66}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MESSAGETABLE', u'offset': 556928, u'sha256': u'ef493afd7e7a330a21862c1623e75eab30b223bf04d434d0e4fe006a2d7faef6', u'type': u'data', u'size': 1720}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 558648, 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': 558684, 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': 558748, u'sha256': u'253d5d8fb2a759cddd1a3a1eeec21a0fd690321242895aafd07c950cb0d08095', u'type': u'data', u'size': 860}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 559608, 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': 560820, u'sha256': u'1a12454cf61b47cb5b00ccd3b5a7e012a81d8225a894f9b73ea60335d6b9d5f1', u'type': u'data', u'size': 93}

{u'lang': u'LANG_NEUTRAL', u'name': u'30', u'offset': 560916, u'sha256': u'cf5260d05db04a6c040dd17131c2114fbafd19b16c2dc5f6803c86135a6f8d0a', u'type': u'data', u'size': 93}

{u'lang': u'LANG_NEUTRAL', u'name': u'30', u'offset': 561012, u'sha256': u'cf5260d05db04a6c040dd17131c2114fbafd19b16c2dc5f6803c86135a6f8d0a', u'type': u'data', u'size': 93}

{u'lang': u'LANG_NEUTRAL', u'name': u'30', u'offset': 561108, u'sha256': u'cf5260d05db04a6c040dd17131c2114fbafd19b16c2dc5f6803c86135a6f8d0a', u'type': u'data', u'size': 93}

{u'lang': u'LANG_NEUTRAL', u'name': u'31', u'offset': 561204, u'sha256': u'8855508aade16ec573d21e6a485dfd0a7624085c1a14b5ecdd6485de0c6839a4', u'type': u'data', u'size': 5}

{u'lang': u'LANG_NEUTRAL', u'name': u'31', u'offset': 561212, 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': 561216, 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': 561220, 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': 561224, 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': 561228, 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': 561232, 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': 609308, 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': 655468, 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': 705792, 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': 753528, 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': 877184, u'sha256': u'a6eb2699548dbaa081439261781a074d12acc6cce4057d6733b37ad8cefed359', u'type': u'data', u'size': 1433}
{u'lang': u'LANG_NEUTRAL', u'name': u'34', u'offset': 878620, 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': 894684, 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': 913276, u'sha256': u'f57c701f8da5a3f48d1864d559c1a6a25ed62044fc536d3cefff33537ea57c99', u'type': u'bzip2 compressed data, block size = 900k', u'size': 5077}
{u'lang': u'LANG_NEUTRAL', u'name': u'34', u'offset': 918356, 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': 921380, 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': 933144, 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)

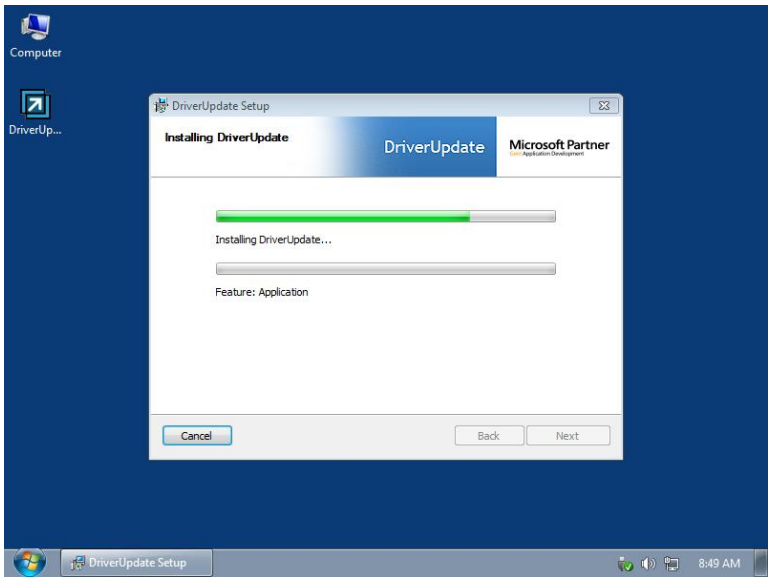
[+] VeriSign Class 3 Code Signing 2010 CA	
Status	NoError ✔
Start Date	2010-02-08 02:00:00
End Date	2020-02-08 01:59:59
Sha256	0f5cd6ebab15fa367e35893fad2bc49cd1a95449f58e7eb978d72bb0b100d764
Serial	5200E5AA2556FC1A86ED96C9D44B33C7
Subject Key Identifier	cf 99 a9 ea 7b 26 f4 4b c9 8e 8f d7 f0 05 26 ef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

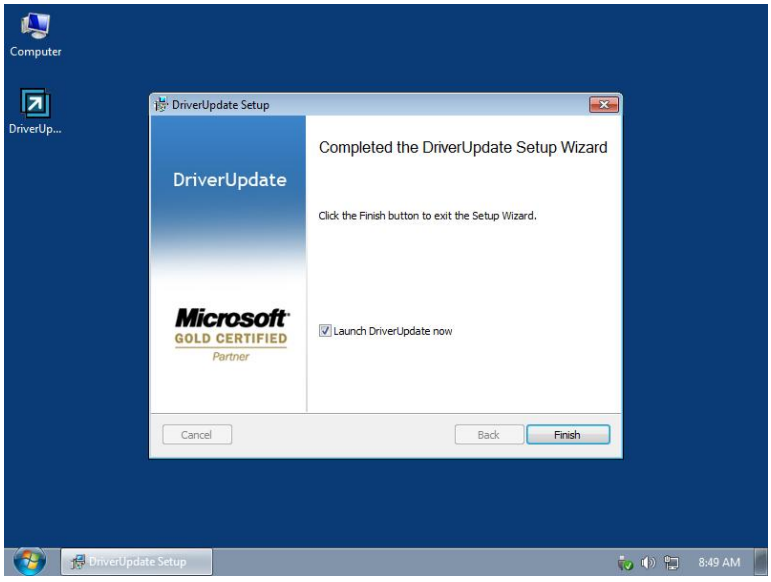
[+] VeriSign Class 3 Public Primary Certification Authority - G5	
Status	NoError ✔
Start Date	2006-11-08 02:00:00
End Date	2036-07-17 02:59:59
Sha256	d0c133d98cabb2199501a761f5b8b9afd30d870477a534b41400a6dc57f5d64d
Serial	18DAD19E267DE8BB4A2158CDCC6B3B4A
Subject Key Identifier	7f d3 65 a7 c2 dd ec bb 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

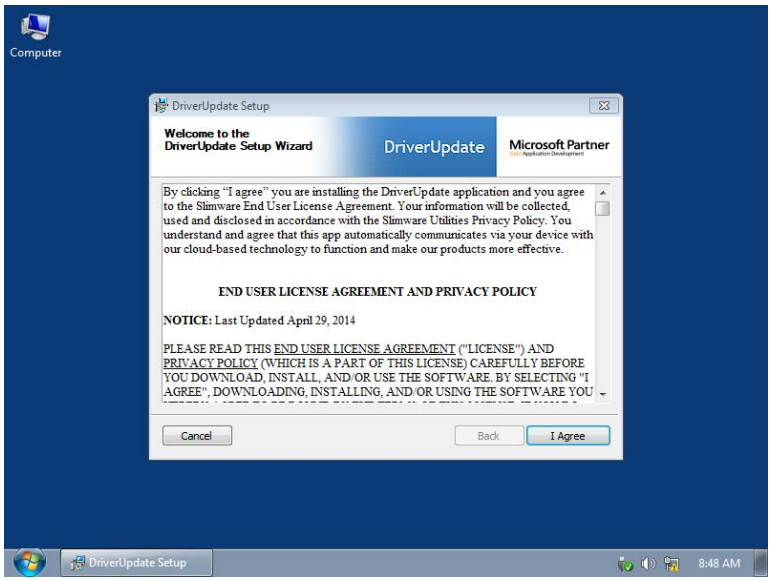
[+] Symantec Time Stamping Services CA - G2	
Status	NoError ✔
Start Date	2012-12-21 02:00:00
End Date	2020-12-31 01:59:59
Sha256	0b44526ab89f4778858bf831045ec218d0d57734caa10208ea3d8c90c1043266
Serial	7E93EBFB7CC64E59EA4B9A77D406FC3B
Subject Key Identifier	5f 9a f5 6e 5c cc cc 74 9a d4 dd 7d ef 3f db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

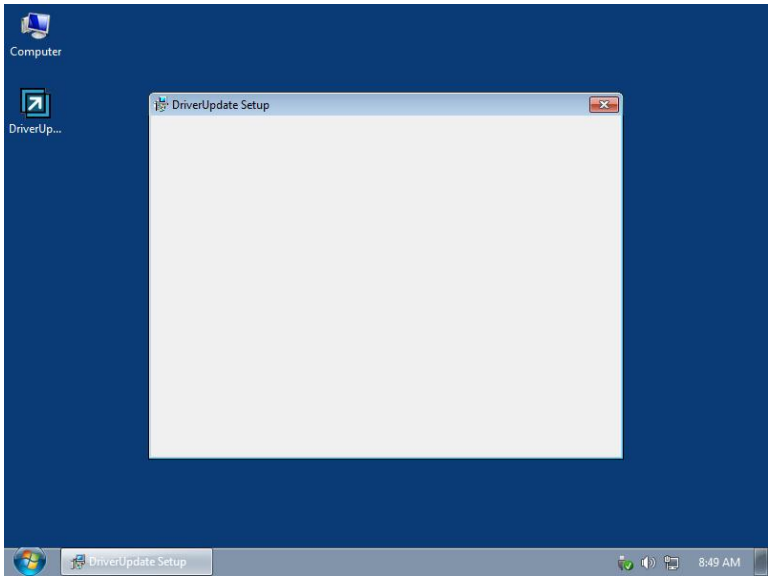
[+] Thawte Timestamping CA	
Status	NoError ✔
Start Date	1997-01-01 02:00:00
End Date	2021-01-01 01:59:59
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Key Identifier	undefined
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Crl link	undefined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

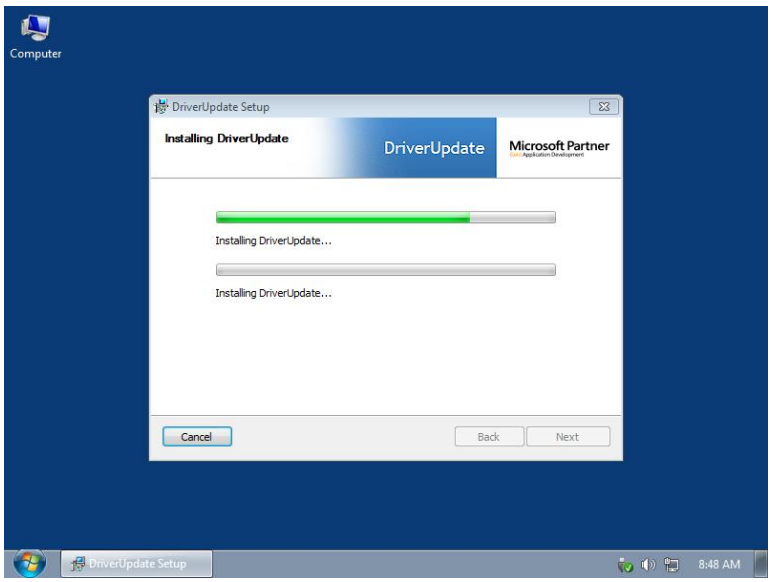
SCREENSHOTS

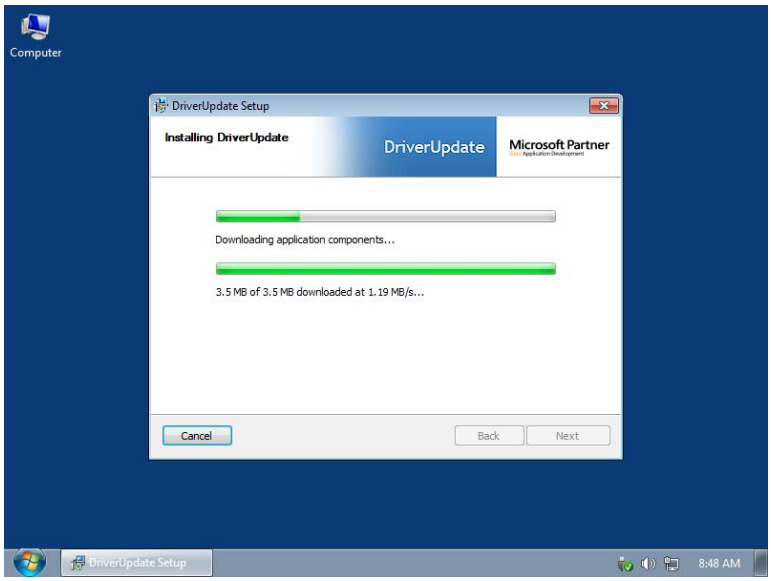




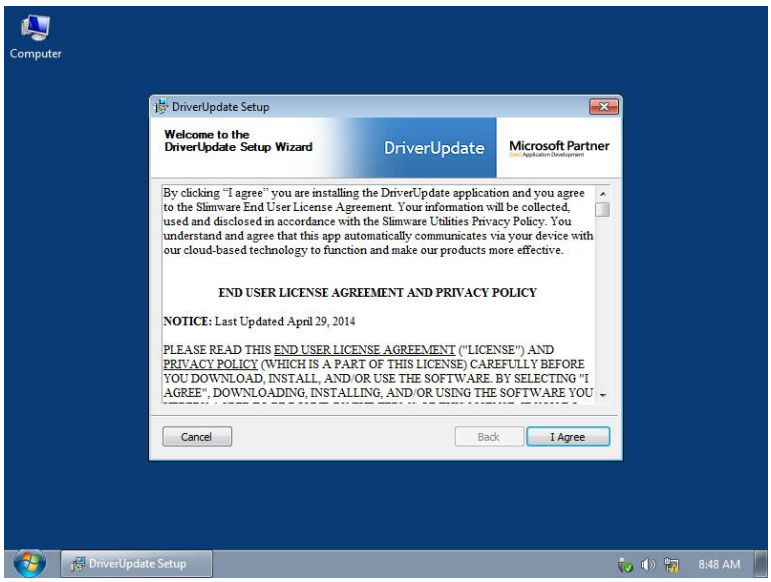

Computer
DriverUpdate Setup
Welcome to the DriverUpdate Setup Wizard
DriverUpdate
Microsoft Partner
By clicking "I agree" you are installing the DriverUpdate application and you agree to the Slimware End User License Agreement. Your information will be collected, used and disclosed in accordance with 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
8:48 AM


Computer
DriverUp...
DriverUpdate Setup
DriverUpdate Setup
8:49 AM


Computer
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Installing DriverUpdate...
Cancel
Back
Next
DriverUpdate Setup
8:48 AM

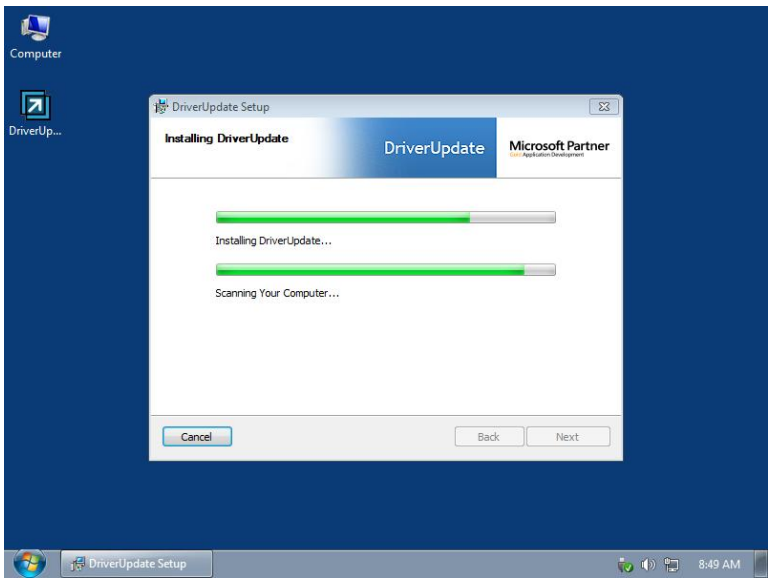

Computer
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Downloading application components...
3.5 MB of 3.5 MB downloaded at 1.19 MB/s...
Cancel
Back
Next
DriverUpdate Setup
8:48 AM

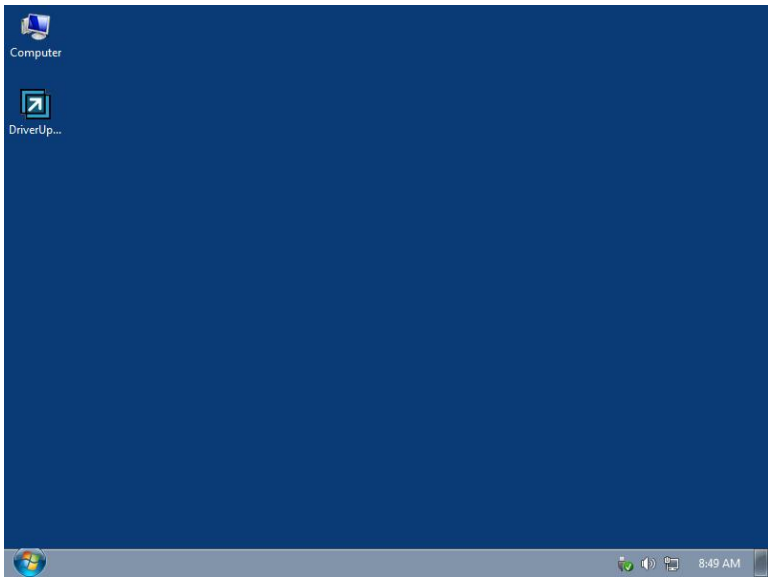

Computer
DriverUp...
SlimClea... Plus
8:49 AM

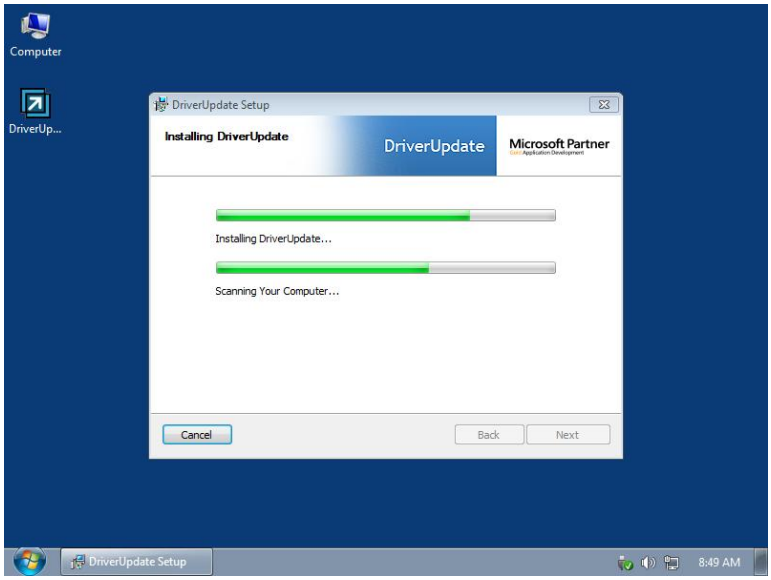

Computer
DriverUpdate Setup
Welcome to the DriverUpdate Setup Wizard
DriverUpdate
Microsoft Partner
By clicking "I agree" you are installing the DriverUpdate application and you agree to the Slimware End User License Agreement. Your information will be collected, used and disclosed in accordance with 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
8:48 AM

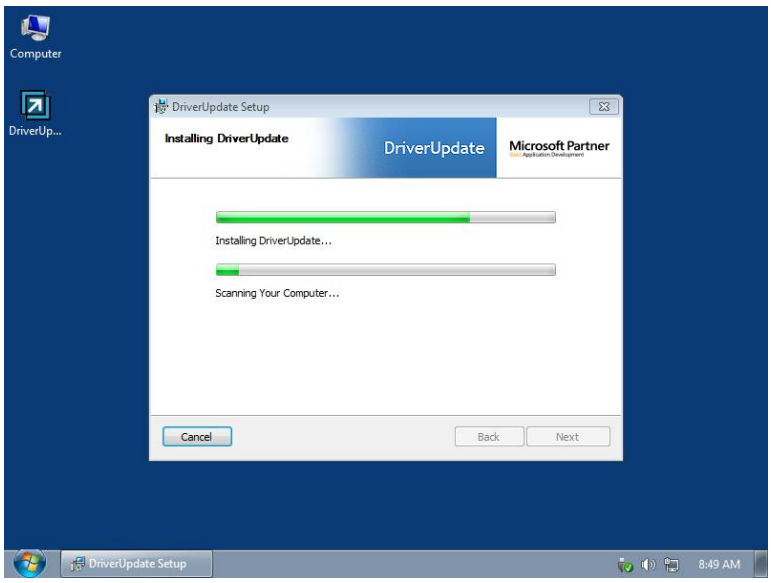

Computer
8:48 AM

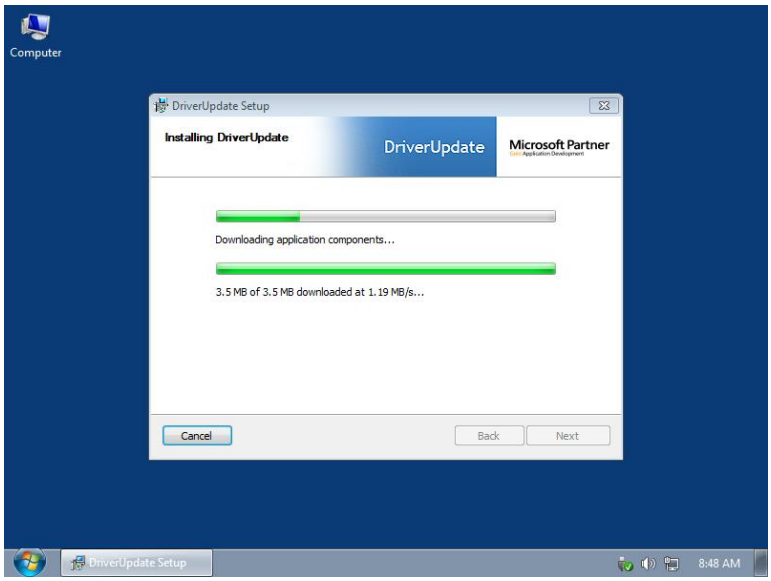

Computer
DriverUp...
SlimClea... Plus
8:50 AM

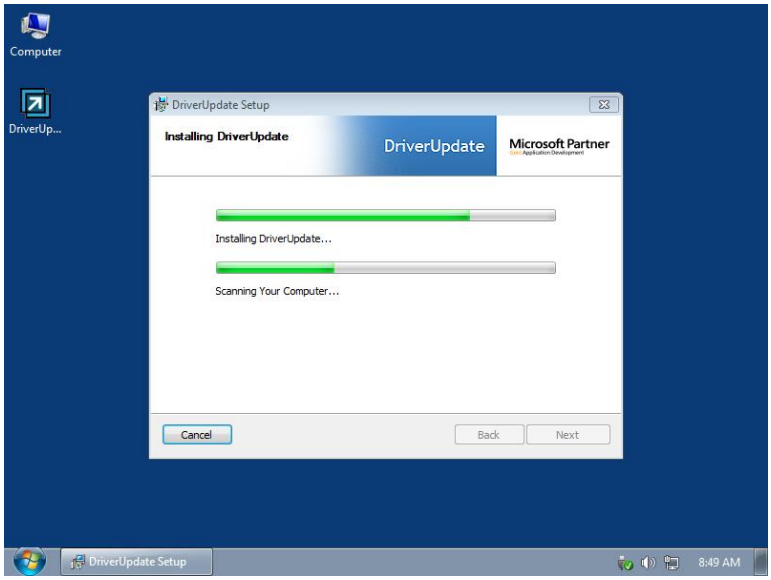

Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Scanning Your Computer...
Cancel
Back
Next
DriverUpdate Setup
8:49 AM


Computer
DriverUp...
8:49 AM

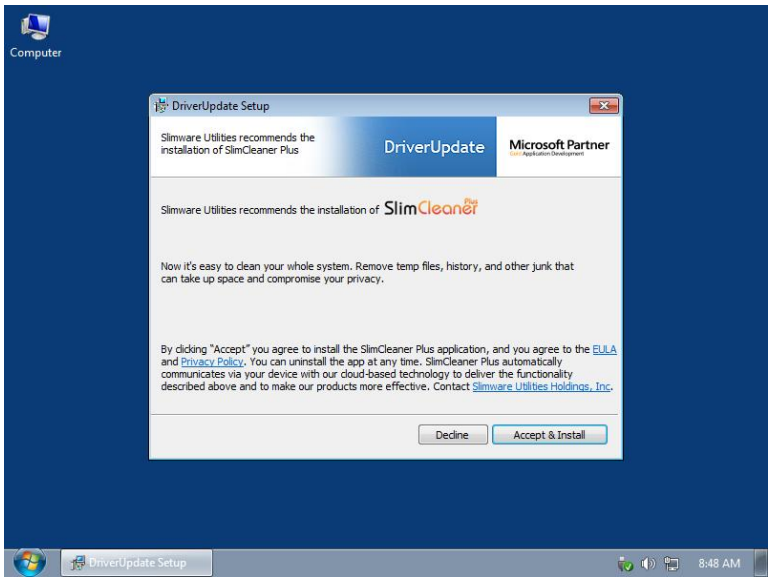

Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Scanning Your Computer...
Cancel
Back
Next
DriverUpdate Setup
8:49 AM


Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Scanning Your Computer...
Cancel
Back
Next
DriverUpdate Setup
8:49 AM


Computer
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Downloading application components...
3.5 MB of 3.5 MB downloaded at 1.19 MB/s...
Cancel
Back
Next
DriverUpdate Setup
8:48 AM


Computer
DriverUp...
DriverUpdate Setup
Installing DriverUpdate
DriverUpdate
Microsoft Partner
Installing DriverUpdate...
Scanning Your Computer...
Cancel
Back
Next
DriverUpdate Setup
8:49 AM


Computer
DriverUp...
SlimClea... Plus
8:50 AM


Computer
DriverUpdate Setup
Slimware Utilities recommends the installation of SlimCleaner Plus
DriverUpdate
Microsoft Partner
Slimware Utilities recommends the installation of SlimCleaner Plus
Now it's easy to clean your whole system. Remove temp files, history, and other junk that can take up space and compromise your privacy.
By clicking "Accept" you agree to install the SlimCleaner Plus application, and you agree to the EULA and Privacy Policy. You can uninstall the app at any time. SlimCleaner Plus automatically communicates via your device with our cloud-based technology to deliver the functionality described above and to make our products more effective. Contact Slimware Utilities Holdings, Inc.
Decline
Accept & Install
DriverUpdate Setup
8:48 AM