virustotal

SHA256:	3b816769f63c9f259e0c883a140d457b0eef99a9f4d9b5cf036192b7668d6a2c
SHA1:	e42d32cbf665dd278076714a677d6209677f1e2f
MD5:	2ec859554451e87a0b1c6d2545e9333e
File size:	431.5 KB (441856 bytes)
File name:	TweakUI.exe
File type:	Win32 EXE
Detection ratio:	0 / 42
Analysis date:	2012-04-07 08:19:45 UTC (0 minute ago)

Antivirus	Result	Update
AhnLab-V3	-	20120406
AntiVir	-	20120406
Antiy-AVL	-	20120407
Avast	-	20120406
AVG	-	20120407
BitDefender	-	20120407
ByteHero	-	20120402
CAT-QuickHeal	-	20120406
ClamAV	-	20120407
Commtouch	-	20120406
Comodo	-	20120407
DrWeb	-	20120407
Emsisoft	-	20120407
eSafe	-	20120405
eTrust-Vet	-	20120406
F-Prot	-	20120406
F-Secure	-	20120407
Fortinet	-	20120407
GData	-	20120407
Ikarus	-	20120407
Jiangmin	-	20120331
K7AntiVirus	-	20120405

Kaspersky	-	20120407
McAfee	-	20120407
McAfee-GW-Edition	-	20120406
Microsoft	-	20120407
NOD32	-	20120407
Norman	-	20120405
nProtect	-	20120407
Panda	-	20120406
PCTools	-	20120407
Prevx	-	20120407
Rising	-	20120406
Sophos	-	20120407
SUPERAntiSpyware	-	20120402
Symantec	-	20120407
TheHacker	-	20120406
TrendMicro	-	20120407
TrendMicro-HouseCall	-	20120407
VBA32	-	20120405
VIPRE	-	20120407
ViRobot	-	20120407

Comments | Additional information

ssdeep

6144:W5vBhGOsKSyVwA351k7VYQFCbTuOlRkZC2TfmDHK:KGOsKJd358BF+uOlReF

TrID

Win32 Executable MS Visual C++ (generic) (65.2%)
Win32 Executable Generic (14.7%)
Win32 Dynamic Link Library (generic) (13.1%)
Generic Win/DOS Executable (3.4%)
DOS Executable Generic (3.4%)

ExifTool

```
UninitializedDataSize....: 0
InitializedDataSize......: 345600
ImageVersion.............: 5.2
ProductName..............: Microsoft   Windows(TM) Shell PowerToys
FileVersionNumber........: 2.10.0.5
LanguageCode.............: French
FileFlagsMask............: 0x003f
FileDescription..........: Interface de r  glages avanc  s de Windows
CharacterSet.............: Windows, Latin1
LinkerVersion............: 7.1
FileOS...................: Windows NT 32-bit
```

```
FileVersion..............: 2.10.0.5
TimeStamp................: 2003:05:13 21:08:15+02:00
FileType.................: Win32 EXE
PEType...................: PE32
InternalName.............: TWEAKUI
ProductVersion...........: 96.02.06
SubsystemVersion.........: 5.1
OSVersion................: 5.2
OriginalFilename.........: TWEAKUI.EXE
LegalCopyright...........: Copyright    Microsoft Corp. 1995-2001
MachineType..............: Intel 386 or later, and compatibles
CompanyName..............: Microsoft Corporation
CodeSize.................: 95232
FileSubtype..............: 0
ProductVersionNumber.....: 96.2.6.0
EntryPoint...............: 0x16361
ObjectFileType...........: Executable application
```

Sigcheck

```
publisher................: Microsoft Corporation
product..................: Microsoft_ Windows(TM) Shell PowerToys
internal name............: TWEAKUI
copyright................: Copyright (c) Microsoft Corp. 1995-2001
original name............: TWEAKUI.EXE
file version.............: 2.10.0.5
description..............: Interface de r_glages avanc_s de Windows
```

Portable Executable structural information

```
Compilation timedatestamp.....: 2003-05-13 19:08:15
Target machine................: 0x14C (Intel 386 or later processors and compatible processors)
Entry point address...........: 0x00016361

PE Sections...................:

Name        Virtual Address  Virtual Size  Raw Size  Entropy  MD5
.text                  4096         94742     95232     6.12  9331be5d9d1ef30eb0d7131c0de17fa1
.data                102400          3176      1536     3.72  1acd4cfeef98750a6e6dba36c6316017
.rsrc                106496        343852    344064     4.72  e7eda9f3ae7693024515d576123ef653

PE Imports...................:

comdlg32.dll
        ChooseColorW, GetOpenFileNameW, GetSaveFileNameW

ACLUI.dll

msvcrt.dll
        _c_exit, _except_handler3, _exit, __set_app_type, __p__fmode, __p__commode, _adjust_fdiv, __setusermatherr,
_initterm, __getmainargs, _acmdln, exit, _cexit, _controlfp, _XcptFilter, _purecall

VERSION.dll
        GetFileVersionInfoW, VerQueryValueW, GetFileVersionInfoSizeW

GDI32.dll
        SetTextColor, GetDeviceCaps, GetObjectW, CreateHalftonePalette, CreatePatternBrush, SelectPalette,
RealizePalette, SetStretchBltMode, SetBkMode, StretchBlt, CreateCompatibleDC, SelectObject, SetBkColor, ExtTextOutW,
DeleteDC, DeleteObject, CreateCompatibleBitmap

COMCTL32.dll
        PropertySheetW, -, -, ImageList_ReplaceIcon, -, ImageList_LoadImageW, -, ImageList_Draw, ImageList_Destroy,
ImageList_Create, ImageList_SetOverlayImage

msi.dll
```

```
ADVAPI32.dll
        RegDeleteKeyW, LsaClose, RegSetKeySecurity, SetFileSecurityW, IsValidSecurityDescriptor, InitializeAcl,
InitializeSecurityDescriptor, MakeSelfRelativeSD, MapGenericMask, GetSecurityDescriptorLength, RegGetKeySecurity,
GetFileSecurityW, AddAccessAllowedAceEx, IsWellKnownSid, FindFirstFreeAce, GetSecurityDescriptorSacl,
SetSecurityDescriptorSacl, RegCloseKey, RegOpenKeyExW, RegCreateKeyExW, RegEnumKeyW, RegSetValueExW, RegQueryValueExW,
LookupAccountSidW, CreateWellKnownSid, RegEnumValueW, RegQueryValueW, RegDeleteValueW, GetUserNameW, LsaStorePrivateData,
LsaOpenPolicy, RevertToSelf, ImpersonateSelf, OpenThreadToken, AreAllAccessesGranted, AccessCheck,
SetSecurityDescriptorOwner, GetSecurityDescriptorOwner, SetSecurityDescriptorGroup, GetSecurityDescriptorGroup,
SetSecurityDescriptorDacl, GetSecurityDescriptorDacl

KERNEL32.dll
        DeleteFileW, GetWindowsDirectoryW, FreeLibrary, LoadLibraryW, MulDiv, CloseHandle, CreateFileW, LocalAlloc,
ExpandEnvironmentStringsW, lstrcmpW, GetTickCount, GetPrivateProfileStringW, WritePrivateProfileStringW, FindClose,
FindNextFileW, FindFirstFileW, SetCurrentDirectoryW, GetSystemDirectoryW, GetCurrentDirectoryW, GetProcAddress,
GetLastError, GetCurrentThread, InterlockedIncrement, InterlockedDecrement, CopyFileW, LockResource, LoadResource,
SizeofResource, FindResourceW, GetSystemWindowsDirectoryW, GetModuleHandleW, WriteFile, GetModuleFileNameW,
GetVersionExW, GetDllDirectoryW, CompareStringW, SetErrorMode, GetStartupInfoA, SetFileAttributesW, GetFileAttributesW,
SearchPathW, GetSystemTime, GetCommandLineW, GetSystemInfo, GetNativeSystemInfo, lstrcmpiW, LocalFree, lstrcpynW,
GetDriveTypeW, lstrcpyW, lstrlenW

UxTheme.dll
        EnableThemeDialogTexture, DrawThemeParentBackground

OLEAUT32.dll
        -, -, -

NETAPI32.dll
        NetApiBufferFree, NetUserModalsGet, NetUserGetLocalGroups, NetQueryDisplayInformation, NetGetJoinInformation

SHELL32.dll
        SHGetFileInfoW, SHChangeNotify, SHGetSpecialFolderLocation, SHGetPathFromIDListW, SHBrowseForFolderW,
ExtractIconW, SHGetFolderPathW, SHGetFolderPathAndSubDirW, SHGetDesktopFolder, ShellExecuteW, ExtractIconExW,
SHGetSpecialFolderPathW, FindExecutableW, -

ntdll.dll
        RtlInitUnicodeString, RtlRunDecodeUnicodeString, RtlRunEncodeUnicodeString

ole32.dll
        CoTaskMemAlloc, CoTaskMemFree, CoTaskMemRealloc, CoUninitialize, CoInitialize, CoCreateInstance, CLSIDFromProgID

SHLWAPI.dll
        SHGetValueW, SHDeleteKeyW, PathCombineW, SHStrDupW, SHSetValueW, wnsprintfW, StrCmpNIW, StrDupW, StrCmpNW,
SHDeleteValueW, StrToIntW, PathGetArgsW, PathParseIconLocationW, SHAutoComplete, PathUnquoteSpacesW, PathRemoveArgsW,
PathQuoteSpacesW, PathFileExistsW, PathAppendW, SHRegGetPathW, SHRegSetPathW, PathFindFileNameW, SHRegGetBoolUSValueW,
StrCatBuffW, AssocQueryStringW, PathRemoveFileSpecW, -, SHQueryValueExW, StrRetToStrW, StrChrW, -, StrStrIW,
PathFindExtensionW, wvnsprintfW, SHCreateStreamOnFileW

USER32.dll
        GetMessagePos, GetKeyState, EnableMenuItem, wsprintfW, DestroyIcon, CharLowerW, GetWindowTextW, GetComboBoxInfo,
DrawFocusRect, DrawIcon, CreateDialogIndirectParamW, MapDialogRect, DrawEdge, GetNextDlgTabItem, PostMessageW, GetFocus,
CharNextW, LoadIconW, MessageBoxW, DestroyMenu, LoadMenuW, SetMenuItemInfoW, GetMessageTime, InflateRect, SetCapture,
IsWindowEnabled, TrackMouseEvent, GetSubMenu, TrackPopupMenuEx, PtInRect, GetIconInfo, ClientToScreen, SetCursorPos,
ReleaseCapture, GetDoubleClickTime, SetFocus, SetWindowPos, SetTimer, KillTimer, LoadImageW, GetDlgCtrlID,
SystemParametersInfoW, GetWindowTextLengthW, SetSysColors, SendNotifyMessageW, GetSysColorBrush, GetSysColor,
GetSystemMetrics, BeginPaint, EndPaint, InvalidateRect, GetClientRect, GetDC, ReleaseDC, LoadCursorW, SetCursor,
DialogBoxParamW, SetWindowLongW, GetWindowLongW, EndDialog, GetDlgItemTextW, GetDlgItemInt, SetDlgItemInt,
SendDlgItemMessageW, CreateWindowExW, CheckRadioButton, IsDlgButtonChecked, CheckDlgButton, BeginDeferWindowPos,
DeferWindowPos, EndDeferWindowPos, GetWindowRect, MapWindowPoints, DestroyWindow, LoadStringW, SetDlgItemTextW,
SetWindowTextW, ShowWindow, EnableWindow, GetParent, SendMessageW, GetDlgItem

OLEACC.dll
        CreateStdAccessibleObject, GetRoleTextW, LresultFromObject
```

Symantec Reputation

Suspicious.Insight

2012-04-07 08:19:45 UTC (3 minutes ago)

Last seen by VirusTotal

2012-04-07 08:19:45 UTC (3 minutes ago)

File names (max. 25)

1. TweakUI.exe