1.0 Summary

Findings and observations:
Remote access trojan coded in Delphi. Extensive functionality to monitor user activity (inputs, files, desktops, remote shells, audio/video equipment). This malware also appears to have capabilities more often related to botnets (such as DDoS capabilities).

Recommendations:
Avoid downloading files hosted publicly on DC hubs (or other P2P services). Don't allow users access to these services without some vetting (e.g., an IT professional may need access to bittorrent in order to obtain Linux ISOs). Keep regular users from running in administrator mode, as there was a bit of lost functionality for the malware in terms of system control when run as a regular user. Blocking the domain max19916.hopto.org would be good, but given the number of shady sites hosted at hopto.org it might be best to simply block the entire domain.

Conclusion:
A very interesting sample, particularly around how it was being distributed. The extent to which one could invade a victim's privacy with this malware was a bit disturbing.

1.1 Identification

File Name: Deadliest Catch S08E07.exe
File Type: Windows 32-bit executable
Malware name(s): Dark Comet
Current detection: 42/49
Malware type: RAT
Size: 674,353 bytes
Packer: None
Encryption/encoding: None definitely detected, though some possible XOR encoding was observed (over 5,000+ XOR statements in the malware precluded a more careful search given available tools)
Origin: Public DC hub located in Eurasia
Compile time: 2012/06/08 Fri 11:12:27Z

Hashes:
```
MD5:be1fa25529308e909381777bcd7f0e92a
SHA1:9a3c2eefb12d527d2d7377a8c6f96854baf566c9
SHA256:d673493ef6288338bace20a165b32b7fb897400e943c7b313a0cef3d1cba22dd
ssdeep:12288:C9HMeUmcufrvA3kb445UEJ2jsWiD4EvFuu4cNgZhCiZKD/XdyF5:uiBIGkbxqEcjsWiDxguehC2SE
```

Test environment details: Win 7 Home Premium SP1 running in VirtualBox 5.0.18_Ubuntu r106667 on Ubuntu 16.04. Hardware is an Acer Aspire 5742 (Intel i3).

1.2 Dependencies

OS: 32-bit Windows
Imports (DLLs):
advapi32.dll
avicap32.dll
comctl32.dll
gdi32.dll
gdiplus.dll
kernel32.dll
msacm32.dll

netapi32.dll
ntdll.dll
ole32.dll
oleaut32.dll
shell32.dll
shfolder.dll
urlmon.dll
user32.dll
version.dll
wininet.dll
winmm.dll
ws2_32.dll
wsock32.dll
Exports: None
Other: N/A

2.0 Characteristics

2.1 Behavior

The file executes and then spawns a number of other processes (two iexplore.exe processes, msdcsc.exe and notepad.exe). The overall functionality allows quite a bit of control over the host computer. This functionality includes a remote shell, keylogging, ability to torrent files, a file download/update process for the malware, access to audio and video equipment available to the victim computer, system inventory, disabling system security features, and DDoS capabilities. The iexplore.exe and notepad.exe processes both have code injected into them. Anti-analysis features appear to be in place, though unconfirmed.

2.2 Infection

The malware's vector was a Windows executable disguised as an episode of a television show found on a public DC hub. Given the nature of the file and its relatively small size, it could also have been delivered via email, via a malicious link, or even via physical means such as a USB key found in a public area (though keeping in mind that it does require execution to infect the host – it will not automatically run on its own).

2.3 Persistence

Changes were observed in the registry that would cause the file to be run at startup, specifically:

As text:

```
HKU\S-1-5-21-2333244481-2062130026-617143801-
1001\Software\Microsoft\Windows\CurrentVersion\Run\MicroUpdate: "C:\Users\Linux
Derp\Documents\MSDCSC\msdcsc.exe"
```

Note that this path is also where the malware makes a copy of itself.

2.4 Movement

None observed.

2.5 Data Exfiltration

Not explicitly observed, though it was seen in the file that there is functionality for uploading files via FTP, which might be how the keylogging files are retrieved by the controller. There is also functionality to view the victim's desktop, view and retrieve contents of their clipboard, view their task manager, and also obtain live audio and video from the victim's machine.

2.6 C²

C2 appears to be controlled from max19916.hopto.org.

2.7 Signatures

File system / host based:
Key added:

```
HKU\S-1-5-21-2333244481-2062130026-617143801-
1001\Software\Microsoft\Windows\CurrentVersion\System
```

Values added:

```
HKU\S-1-5-21-2333244481-2062130026-617143801-
1001\Software\Microsoft\Windows\CurrentVersion\Run\MicroUpdate: "C:\Users\Linux
Derp\Documents\MSDCSC\msdcsc.exe"
HKU\S-1-5-21-2333244481-2062130026-617143801-
1001\Software\Microsoft\Windows\CurrentVersion\System\DisableRegistryTools: 0x00000001
HKU\S-1-5-21-2333244481-2062130026-617143801-
1001\Software\Microsoft\Windows\CurrentVersion\System\EnableLUA: 0x00000000
```

Successful only when run as admin:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CurrentVersion\Explorern\NoControlPa
nel: "1"
HKLM\SOFTWARE\Wow6432Node\Microsoft\Security Center\AntiVirusDisableNotify: "1"
HKLM\SOFTWARE\Wow6432Node\Microsoft\Security Center\UpdatesDisableNotify: "1"
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\CurrentVersion\Explorern
\NoControlPanel: "1"
```

Files added:

```
c:\Users\Linux Derp\AppData\Roaming\dclogs\2016-08-31-4.dc
c:\Users\Linux Derp\Documents\MSDCSC\msdcsc.exe
```

```
Note that the directory and extension for the log file remains constant, while the file
names are dynamically generated based on the pattern observed of YYYY-MM-DD-[serial
number].dc. The malware always installs itself at the msdcsc.exe file name and path as
shown, at least during these runs. There appears to be a capability to install to a randomly
generated directory, though this was not observed taking place.
```

Network based:
- Traffic / domain resolution for max19916.hopto.org

3.0 Raw Notes

```
Strings (cleaned up version):
Strings v2.51
Copyright (C) 1999-2013 Mark Russinovich
Sysinternals - www.sysinternals.com

MZP
This program must be run under Win32
.text
`.itext
`.data
.bss
.idata
.tls
.rdata
@.reloc
B.rsrc
Boolean
FALSE
TRUE
Char
Integer
Byte
Word
Cardinal
string
WideString
OleVariant
TObject
TObject
System
IInterface
System
IDispatch4
System
TInterfacedObject
FastMM Borland Edition
 2004, 2005 Pierre le Riche / Professional Software Development
An unexpected memory leak has occurred.
The unexpected small block leaks are:
 bytes:
Unknown
String
The sizes of unexpected leaked medium and large blocks are:
Unexpected Memory Leak
SOFTWARE\Borland\Delphi\RTL
FPUMaskValue
kernel32.dll
GetLongPathNameA
Software\Borland\Locales
Software\Borland\Delphi\Locales
odSelected
odGrayed
odDisabled
odChecked
odFocused
odDefault
odHotLight
odInactive
odNoAccel
odNoFocusRect
odReserved1
odReserved2
odComboBoxEdit
```

Windows
TOwnerDrawState
Magellan MSWHEEL
MouseZ
MSWHEEL_ROLLMSG
MSH_WHEELSUPPORT_MSG
MSH_SCROLL_LINES_MSG
tagMULTI_QI
IPersist4
ActiveX
tagEXCEPINFO
TFileName
TSearchRec`
Exception
EAbort
EHeapException
EOutOfMemory
EInOutErrorH
EExternal
EExternalException
EIntError
EDivByZero
ERangeError
EIntOverflow
EMathError
EInvalidOp
EZeroDividel
EOverflow
EUnderflow
EInvalidPointerx
EInvalidCast
EConvertError
EAccessViolation
EPrivilege
EStackOverflow
EControlC
EVariantError
EAssertionFailed
EAbstractError
EIntfCastError
EOSError
ESafecallException
0.74
SysUtils
0.84
SysUtils
TThreadLocalCounter
$TMultiReadExclusiveWriteSynchronizer
TRUE
FALSE
$*@@@*$@@@$ *@@* $@@($*)@-$*@@$-*@@$*-@@(*$)@-*$@@*-$@@*$-@@-* $@-$ *@* $-@$ *-@$ -*@*- $@($
)(TErrorRec
TExceptRec
m/d/yy
mmmm d, yyyy
 AMPM
AMPM
:mm:ss
TUnitHashArray
SysUtils
TModuleInfo
kernel32.dll
GetDiskFreeSpaceExA
oleaut32.dll
VariantChangeTypeEx
VarNeg

VarNot
VarAdd
VarSub
VarMul
VarDiv
VarIdiv
VarMod
VarAnd
VarOr
VarXor
VarCmp
VarI4FromStr
VarR4FromStr
VarR8FromStr
VarDateFromStr
VarCyFromStr
VarBoolFromStr
VarBstrFromCy
VarBstrFromDate
VarBstrFromBool
TCustomVariantType
TCustomVariantType
Variants
EVariantInvalidOpError
EVariantTypeCastError
EVariantOverflowError
EVariantInvalidArgError
EVariantBadVarTypeErrorX
EVariantBadIndexError
EVariantArrayLockedError
EVariantArrayCreateError
EVariantNotImplError
EVariantOutOfMemoryError
EVariantUnexpectedError
EVariantDispatchError
Empty
Null
Smallint
Integer
Single
Double
Currency
Date
OleStr
Dispatch
Error
Boolean
Variant
Unknown
Decimal
ShortInt
Byte
Word
LongWord
Int64
String
Any
Array
ByRef
0.02
Variants
TBiDiMode
bdLeftToRight
bdRightToLeft
bdRightToLeftNoAlign
bdRightToLeftReadingOnly

Classes
ssShift
ssAlt
ssCtrl
ssLeft
ssRight
ssMiddle
ssDouble
Classes
TShiftState
THelpContext
THelpType
htKeyword
htContext
ClassesHmA
TShortCut
TNotifyEvent
Sender
TObject
EStreamError
EFileStreamError
EFCreateError
EFOpenErrorDoA
EFilerError
EReadError
EWriteErrorLpA
EClassNotFound
EResNotFound
EListError
EBitsError
EStringListError
EComponentErrorprA
EOutOfResources
EInvalidOperation
TList
TThreadList
TBits
TPersistent
TPersistent<tA
Classes
TInterfacedPersistenthuA
TInterfacedPersistent,uA
Classes
IStringsAdapter4
Classes
TStrings
TStrings
Classes
TStringItem
TStringList
TStringListPwA
Classes
TStream
THandleStream
TFileStream
TCustomMemoryStreamTzA
TMemoryStream
TStringStreamX{A
TResourceStream
TStreamAdapter
TClassFinder
TFiler
TReader
EThread
TThread(
TComponentName<

IDesignerNotify4
Classes
TComponent
TComponentd
Classes
Name<
Tag
TBasicActionLink
TBasicAction
TBasicActionD
Classes
TIdentMapEntry
TRegGroup
TRegGroups
TIntConst
Strings
TPropFixup
TPropIntfFixup
Owner
0.56
Classes
FALSE
TRUE
nil
Null
TPUtilWindow
ERegistryException
TRegistryS
EInvalidGraphic4)B
EInvalidGraphicOperation
TFontPitch
fpDefault
fpVariable
fpFixed
Graphics
TFontName
TFontCharset
TFontStyle
fsBold
fsItalic
fsUnderline
fsStrikeOut
Graphics
TFontStyles
TPenStyle
psSolid
psDash
psDot
psDashDot
psDashDotDot
psClear
psInsideFrame
psUserStyle
psAlternate
Graphics
TPenMode
pmBlack
pmWhite
pmNop
pmNot
pmCopy
pmNotCopy
pmMergePenNot
pmMaskPenNot
pmMergeNotPen
pmMaskNotPen

pmMerge
pmNotMerge
pmMask
pmNotMask
pmXor
pmNotXor
Graphics
TBrushStyle
bsSolid
bsClear
bsHorizontal
bsVertical
bsFDiagonal
bsBDiagonal
bsCross
bsDiagCross
Graphics
TGraphicsObjectT,B
TGraphicsObject,,B
Graphics
IChangeNotifier4
Graphics
TFont0-B
TFont
Graphics
Charsett(B
Color<
Height
Name<
OrientationP)B
Pitch<
Size
Style
TPen
TPen
Graphics
Color
Mode(*B
Style<
Width
TBrush
TBrush
Graphics
Colord+B
Style
TCanvas
TCanvasd0B
Graphics
Brush<
CopyMode,-B
Font
Pen
TGraphic
TGraphic
Graphics
TPicture
TPicture@3B
Graphics
TSharedImage
TMetafileImage
TMetafile
TMetafile
Graphics
TBitmapImage
TBitmapp6B
TBitmap

Graphics
TIconImage
TIcon
TIcon87B
Graphics
TResourceManager
TBrushResourceManager
clBlack
clMaroon
clGreen
clOlive
clNavy
clPurple
clTeal
clGray
clSilver
clRed
clLime
clYellow
clBlue
clFuchsia
clAqua
clWhite
clMoneyGreen
clSkyBlue
clCream
clMedGray
clActiveBorder
clActiveCaption
clAppWorkSpace
clBackground
clBtnFace
clBtnHighlight
clBtnShadow
clBtnText
clCaptionText
clDefault
clGradientActiveCaption
clGradientInactiveCaption
clGrayText
clHighlight
clHighlightText
clHotLight
clInactiveBorder
clInactiveCaption
clInactiveCaptionText
clInfoBk
clInfoText
clMenu
clMenuBar
clMenuHighlight
clMenuText
clNone
clScrollBar
cl3DDkShadow
cl3DLight
clWindow
clWindowFrame
clWindowText
ANSI_CHARSET
DEFAULT_CHARSET
SYMBOL_CHARSET
MAC_CHARSET
SHIFTJIS_CHARSET
HANGEUL_CHARSET
JOHAB_CHARSET

GB2312_CHARSET
CHINESEBIG5_CHARSET
GREEK_CHARSET
TURKISH_CHARSET
HEBREW_CHARSET
ARABIC_CHARSET
BALTIC_CHARSET
RUSSIAN_CHARSET
THAI_CHARSET
EASTEUROPE_CHARSET
OEM_CHARSET
Default
TClipboardFormats
Data
.wmf
TBitmapCanvas
TBitmapCanvas
Graphics
Tahoma
SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
MS Shell Dlg 2
TPatternManagerSV
TGdiplusBase
TGPImage
TGPBitmap
TGPGraphicsRP
image/jpeg
image/bmp
EOleError
EOleSysError
EOleException
Apartment
Free
Both
Neutral
%s, ClassID: %s
%s, ProgID: "%s"
ole32.dll
CoCreateInstanceEx
CoInitializeEx
CoAddRefServerProcess
CoReleaseServerProcess
CoResumeClassObjects
CoSuspendClassObjects
TUploadFTP
notepad
kernel32.dll
user32.dll
Sleep
MessageBoxA
ExitThread
DeleteFileA
GetLastError
TerminateProcess
CloseHandle
OpenProcess
GetExitCodeProcess
LoadLibraryA
kernel32
GetProcAddress
notepad
DCPERSFWBP
kernel32.dll
user32.dll
Sleep
MessageBoxA

CreateProcessA
GetLastError
SetLastError
CreateMutexA
CloseHandle
ExitThread
OpenProcess
TerminateProcess
GetExitCodeProcess
WaitForSingleObject
LoadLibraryA
kernel32
GetProcAddress
user32
kernel32.dll
CreateToolhelp32Snapshot
Heap32ListFirst
Heap32ListNext
Heap32First
Heap32Next
Toolhelp32ReadProcessMemory
Process32First
Process32Next
Process32FirstW
Process32NextW
Thread32First
Thread32Next
Module32First
Module32Next
Module32FirstW
Module32NextW
-.-.-.-
[::]
need dictionary
stream end
file error
stream error
data error
insufficient memory
buffer error
incompatible version
1.2.3
1.2.3
>:\$
TByteArray
TACMConvertor
TACMIn
TPUtilWindow
BuildImportTable: can't load library:
BuildImportTable: ReallocMemory failed
BuildImportTable: GetProcAddress failed
FinalizeSections: VirtualProtect failed
BTMemoryLoadLibary: dll dos header is not valid
BTMemoryLoadLibary: IMAGE_NT_SIGNATURE is not valid
BTMemoryLoadLibary: VirtualAlloc failed
 BTMemoryLoadLibary: BuildImportTable failed
BTMemoryLoadLibary: Get DLLEntyPoint failed
BTMemoryLoadLibary: Can't attach library
BTMemoryGetProcAddress: no export table found
BTMemoryGetProcAddress: DLL doesn't export anything
BTMemoryGetProcAddress: exported symbol not found
BTMemoryGetProcAddress: name <-> ordinal number don't match
127.0.0.1
TSynchroObject
THandleObject
TEvent

TCriticalSection
OleMainThreadWndClass
tGWh
ole32.dll
CoWaitForMultipleHandles
IPin4
DirectShow9
IFilterGraph4
DirectShow9
IMediaFilter4
DirectShow9
IBaseFilterP
DirectShow9
IGraphBuilder
DirectShow9
ICaptureGraphBuilder24
DirectShow9
IAMStreamConfig4
DirectShow9
IAMVideoProcAmp4
DirectShow9
IKsPropertySet4
DirectShow9
IMediaControld
DirectShow9
IMediaEventd
DirectShow9
IMediaEventEx$
DirectShow9
IVideoWindowd
DirectShow9'
ISampleGrabberCB4
DirectShow9
ISampleGrabber4
DirectShow9
TApplication
TSampleGrabberCBInt
VSample
TSampleGrabberCBImpl
TSampleGrabberCB
VSample
TVideoSample
FriendlyName
FriendlyName
Video Capture
Sample Grabber
Null Renderer
VFramesh
TVideoImage
NewFrame
Unknown compression
DataSize:
  FourCC:
TDCWebCam
TRemoteShell
COMSPEC
wlanapi.dll
WlanOpenHandle
WlanCloseHandle
WlanEnumInterfaces
WlanQueryInterface
WlanGetAvailableNetworkList
80211_OPEN
80211_SHARED_KEY
WPA_PSK
WPA_NONE

RSNA
RSNA_PSK
IHV_START
IHV_END
NONE
WEP40
TKIP
CCMP
WEP104
WPA_USE_GROUP OR RSN_USE_GROUP
IHV_START
IHV_END
TByteArray
UntFWB
\Internet Explorer\iexplore.exe
explorer.exe
TOrderedList
TStack
IHelpSelector4
HelpIntfs
IHelpSystem4
HelpIntfs
ICustomHelpViewer4
HelpIntfs
IExtendedHelpViewerl
HelpIntfs
EHelpSystemException
THelpManager
THelpViewerNode
GetMonitorInfoA
GetSystemMetrics
MonitorFromRect
MonitorFromWindow
MonitorFromPoint
GetMonitorInfo
DISPLAY
GetMonitorInfoA
DISPLAY
GetMonitorInfoW
DISPLAY
EnumDisplayMonitors
USER32.DLL
BeginBufferedPaint
EndBufferedPaint
BufferedPaintSetAlpha
uxtheme.dll
OpenThemeData
CloseThemeData
DrawThemeBackground
DrawThemeText
GetThemeBackgroundContentRect
GetThemePartSize
GetThemeTextExtent
GetThemeTextMetrics
GetThemeBackgroundRegion
HitTestThemeBackground
DrawThemeEdge
DrawThemeIcon
IsThemePartDefined
IsThemeBackgroundPartiallyTransparent
GetThemeColor
GetThemeMetric
GetThemeString
GetThemeBool
GetThemeInt
GetThemeEnumValue

GetThemePosition
GetThemeFont
GetThemeRect
GetThemeMargins
GetThemeIntList
GetThemePropertyOrigin
SetWindowTheme
GetThemeFilename
GetThemeSysColor
GetThemeSysColorBrush
GetThemeSysBool
GetThemeSysSize
GetThemeSysFont
GetThemeSysString
GetThemeSysInt
IsThemeActive
IsAppThemed
GetWindowTheme
EnableThemeDialogTexture
IsThemeDialogTextureEnabled
GetThemeAppProperties
SetThemeAppProperties
GetCurrentThemeName
GetThemeDocumentationProperty
DrawThemeParentBackground
EnableTheming
DWMAPI.DLL
DwmExtendFrameIntoClientArea
DWMAPI.DLL
DwmIsCompositionEnabled
clWebSnow
clWebFloralWhite
clWebLavenderBlush
clWebOldLace
clWebIvory
clWebCornSilk
clWebBeige
clWebAntiqueWhite
clWebWheat
clWebAliceBlue
clWebGhostWhite
clWebLavender
clWebSeashell
clWebLightYellow
clWebPapayaWhip
clWebNavajoWhite
clWebMoccasin
clWebBurlywood
clWebAzure
clWebMintcream
clWebHoneydew
clWebLinen
clWebLemonChiffon
clWebBlanchedAlmond
clWebBisque
clWebPeachPuff
clWebTan
clWebYellow
clWebDarkOrange
clWebRed
clWebDarkRed
clWebMaroon
clWebIndianRed
clWebSalmon
clWebCoral
clWebGold

clWebTomato
clWebCrimson
clWebBrown
clWebChocolate
clWebSandyBrown
clWebLightSalmon
clWebLightCoral
clWebOrange
clWebOrangeRed
clWebFirebrick
clWebSaddleBrown
clWebSienna
clWebPeru
clWebDarkSalmon
clWebRosyBrown
clWebPaleGoldenrod
clWebLightGoldenrodYellow
clWebOlive
clWebForestGreen
clWebGreenYellow
clWebChartreuse
clWebLightGreen
clWebAquamarine
clWebSeaGreen
clWebGoldenRod
clWebKhaki
clWebOliveDrab
clWebGreen
clWebYellowGreen
clWebLawnGreen
clWebPaleGreen
clWebMediumAquamarine
clWebMediumSeaGreen
clWebDarkGoldenRod
clWebDarkKhaki
clWebDarkOliveGreen
clWebDarkgreen
clWebLimeGreen
clWebLime
clWebSpringGreen
clWebMediumSpringGreen
clWebDarkSeaGreen
clWebLightSeaGreen
clWebPaleTurquoise
clWebLightCyan
clWebLightBlue
clWebLightSkyBlue
clWebCornFlowerBlue
clWebDarkBlue
clWebIndigo
clWebMediumTurquoise
clWebTurquoise
clWebCyan
clWebPowderBlue
clWebSkyBlue
clWebRoyalBlue
clWebMediumBlue
clWebMidnightBlue
clWebDarkTurquoise
clWebCadetBlue
clWebDarkCyan
clWebTeal
clWebDeepskyBlue
clWebDodgerBlue
clWebBlue
clWebNavy

clWebDarkViolet
clWebDarkOrchid
clWebMagenta
clWebDarkMagenta
clWebMediumVioletRed
clWebPaleVioletRed
clWebBlueViolet
clWebMediumOrchid
clWebMediumPurple
clWebPurple
clWebDeepPink
clWebLightPink
clWebViolet
clWebOrchid
clWebPlum
clWebThistle
clWebHotPink
clWebPink
clWebLightSteelBlue
clWebMediumSlateBlue
clWebLightSlateGray
clWebWhite
clWebLightgrey
clWebGray
clWebSteelBlue
clWebSlateBlue
clWebSlateGray
clWebWhiteSmoke
clWebSilver
clWebDimGray
clWebMistyRose
clWebDarkSlateBlue
clWebDarkSlategray
clWebGainsboro
clWebDarkGray
clWebBlack
TTimer
TTimerx
ExtCtrls
Enabled|
Interval\mA
OnTimerSV
TCommonDialog
TCommonDialog
Dialogs
Ctl3D
HelpContext\mA
OnClose\mA
OnShowSV
Cancel
Abort
Retry
Ignore
NoToAll
YesToAll
Help
commdlg_help
commdlg_FindReplace
WndProcPtr%.8X%.8X
Err:509
THintActionh
THintAction
StdActns
Hint
comctl32.dll
InitializeFlatSB

UninitializeFlatSB
FlatSB_GetScrollProp
FlatSB_SetScrollProp
FlatSB_EnableScrollBar
FlatSB_ShowScrollBar
FlatSB_GetScrollRange
FlatSB_GetScrollInfo
FlatSB_GetScrollPos
FlatSB_SetScrollPos
FlatSB_SetScrollInfo
FlatSB_SetScrollRange
ZYYd
TThemeServices
Theme manager
 2001, 2002 Mike Lischke
button
clock
combobox
edit
explorerbar
header
listview
menu
page
progress
rebar
scrollbar
spin
startpanel
status
taskband
taskbar
toolbar
tooltip
trackbar
traynotify
treeview
window
BDSUnthemedDesigner
comctl32.dll
ZYYd
ZYYd
EMenuError
TMenuBreak
mbNone
mbBreak
mbBarBreak
Menus
TMenuChangeEvent
Sender
TObject
Source
TMenuItem
Rebuild
Boolean
TMenuDrawItemEvent
Sender
TObject
ACanvas
TCanvas
ARect
TRect
Selected
Boolean
TAdvancedMenuDrawItemEvent
Sender

TObject
ACanvas
TCanvas
ARect
TRect
State
TOwnerDrawState
TMenuMeasureItemEvent
Sender
TObject
ACanvas
TCanvas
Width
Integer
Height
Integer
TMenuItemAutoFlag
maAutomatic
maManual
maParent
Menus
TMenuAutoFlag
Menus
TMenuActionLinkH#D
TMenuItem
TMenuItemH#D
Menus
Action
AutoCheck
AutoHotkeys
AutoLineReductionl6B
Bitmap
Break
Caption
Checked
SubMenuImages
Default
EnabledT
GroupIndex
HelpContext
Hint
ImageIndex
RadioItemDmA
ShortCut
Visible\mA
OnClick` D
OnDrawItem
OnAdvancedDrawItemD!D
OnMeasureItem
TMenu
TMenul'D
Menus
Items
TMainMenu
TMainMenuh(D
Menus
AutoHotkeys
AutoLineReduction
AutoMerge
BiDiMode
Images
OwnerDraw
ParentBiDiMode
OnChange
TPopupAlignment
paLeft

paRight
paCenter
Menus@*D
TTrackButton
tbRightButton
tbLeftButton
Menus
TMenuAnimations
maLeftToRight
maRightToLeft
maTopToBottom
maBottomToTop
maNone
Menus
TMenuAnimation
TPopupMenu
TPopupMenuL+D
Menus
Alignment
AutoHotkeys
AutoLineReduction
AutoPopup
BiDiMode
HelpContext
Images
MenuAnimation
OwnerDraw
ParentBiDiMode<*D
TrackButton
OnChange\mA
OnPopup
TPopupList
TMenuItemStack
1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ
ShortCutText
\SYSTEM\CurrentControlSet\Control\Keyboard Layouts\
Layout File
KbdLayerDescriptor
TCursor
TAlign
alNone
alTop
alBottom
alLeft
alRight
alClient
alCustom
Controls
TDragObject
TDragObject
Controls
TBaseDragControlObject
TBaseDragControlObjectX
Controls
TDragControlObject
TDragControlObjectEx
TDragDockObject
TDragDockObject8
Controls
TDragDockObjectEx
TControlCanvas
TControlCanvas
Controls
TCustomControlAction
TCustomControlAction@
Controls

TControlActionLink
TMouseButton
mbLeft
mbRight
mbMiddle
Controls
TMouseActivate
maDefault
maActivate
maActivateAndEat
maNoActivate
maNoActivateAndEat
Controls
TDragMode
dmManual
dmAutomatic
Controls
TDragState
dsDragEnter
dsDragLeave
dsDragMove
Controls
TDragKind
dkDrag
dkDock
Controls
TCaption
TAnchorKind
akLeft
akTop
akRight
akBottom
Controls
TAnchors
TConstraintSize
TSizeConstraints
TSizeConstraints
Controls
MaxHeight
MaxWidth
MinHeight
MinWidth
TMarginSize
TMargins
TMargins`
Controls
Left
Right
Bottom
TPadding
TPaddingx
Controls
Left
Right
Bottom
TMouseEvent
Sender
TObject
Button
TMouseButton
Shift
TShiftState
Integer
Integer
TMouseMoveEvent
Sender

TObject
Shift
TShiftState
Integer
Integer
TMouseActivateEvent
Sender
TObject
Button
TMouseButton
Shift
TShiftState
Integer
Integer
HitTest
Integer
MouseActivate
TMouseActivate
TKeyEvent
Sender
TObject
Word
Shift
TShiftState
TKeyPressEvent
Sender
TObject
Char
TDragOverEvent
Sender
TObject
Source
TObject
Integer
Integer
State
TDragState
Accept
Boolean
TDragDropEvent
Sender
TObject
Source
TObject
Integer
Integer
TEndDragEvent
Sender
TObject
Target
TObject
Integer
Integer
TDockDropEvent
Sender
TObject
Source
TDragDockObject
Integer
Integer
TDockOverEvent
Sender
TObject
Source
TDragDockObject
Integer

Integer
State
TDragState
Accept
Boolean
TUnDockEvent
Sender
TObject
Client
TControl
NewTarget
TWinControl
Allow
Boolean
TStartDockEvent
Sender
TObject
DragObject
TDragDockObject
TGetSiteInfoEvent
Sender
TObject
DockClient
TControl
InfluenceRect
TRect
MousePos
TPoint
CanDock
Boolean
TCanResizeEvent
Sender
TObject
NewWidth
Integer
NewHeight
Integer
Resize
Boolean
TConstrainedResizeEvent
Sender
TObject
MinWidth
Integer
MinHeight
Integer
MaxWidth
Integer
MaxHeight
Integer
TMouseWheelEvent
Sender
TObject
Shift
TShiftState
WheelDelta
Integer
MousePos
TPoint
Handled
Boolean
TMouseWheelUpDownEvent
Sender
TObject
Shift
TShiftState

MousePos
TPoint
Handled
Boolean
TContextPopupEvent
Sender
TObject
MousePos
TPoint
Handled
Boolean
TControl
TControl
Controls
AlignWithMargins<
Left<
Top<
Width<
Height
Cursor
Hint
HelpType
HelpKeyword
HelpContext
Margins
TWinControlActionLink
TImeName
TBorderWidth
IDockManager4
Controls
TAlignInsertBeforeEvent
Sender
TWinControl
TControl
TControl
Boolean
TAlignPositionEvent
Sender
TWinControl
Control
TControl
NewLeft
Integer
NewTop
Integer
NewWidth
Integer
NewHeight
Integer
AlignRect
TRect
AlignInfo
TAlignInfo
TWinControl
TWinControl
Controls
TCustomControl
TCustomControl
Controls
THintWindow
THintWindow
Controls
TDockZone
TDockTree
TMouse
crDefault

crArrow
crCross
crIBeam
crSizeNESW
crSizeNS
crSizeNWSE
crSizeWE
crUpArrow
crHourGlass
crDrag
crNoDrop
crHSplit
crVSplit
crMultiDrag
crSQLWait
crNo
crAppStart
crHelp
crHandPoint
crSizeAll
crSize
TSiteList
%s (%s)
IsControl
ExplicitLeft
ExplicitTop
ExplicitWidth
ExplicitHeight
DesignSize
USER32
WINNLSEnableIME
imm32.dll
ImmGetContext
ImmReleaseContext
ImmGetConversionStatus
ImmSetConversionStatus
ImmSetOpenStatus
ImmSetCompositionWindow
ImmSetCompositionFontA
ImmGetCompositionStringA
ImmIsIME
ImmNotifyIME
Delphi%.8X
ControlOfs%.8X%.8X
USER32
AnimateWindow
TChangeLink
TImageIndex
TCustomImageList
TCustomImageList
ImgList
comctl32.dll
comctl32.dll
ImageList_WriteEx
TContainedAction
TContainedAction
ActnList
Category
TCustomActionListL
TCustomActionList
ActnList
TShortCutList
TShortCutList
ActnList
TCustomAction
TCustomAction

ActnList
TActionLinkSV
TScrollBarInc
TScrollBarStyle
ssRegular
ssFlat
ssHotTrack
FormsP
TControlScrollBar
TControlScrollBarP
Forms
ButtonSizet(B
Color
Incrementh
Margin
ParentColor<
Position<
Range
Smooth<
Size
Style<
ThumbSize
Tracking
Visible
TWindowState
wsNormal
wsMinimized
wsMaximized
Forms
TScrollingWinControl
TScrollingWinControl
Forms
OnAlignInsertBeforeh
OnAlignPositionp
HorzScrollBarp
VertScrollBar
TFormBorderStyle
bsNone
bsSingle
bsSizeable
bsDialog
bsToolWindow
bsSizeToolWin
FormsL
IDesignerHook8
Forms
IOleForm4
Forms
TPopupWndArray
Forms
TFormStyle
fsNormal
fsMDIChild
fsMDIForm
fsStayOnTop
Forms
TBorderIcon
biSystemMenu
biMinimize
biMaximize
biHelp
Forms
TBorderIcons
TPosition
poDesigned
poDefault

poDefaultPosOnly
poDefaultSizeOnly
poScreenCenter
poDesktopCenter
poMainFormCenter
poOwnerFormCenter
Forms0
TDefaultMonitor
dmDesktop
dmPrimary
dmMainForm
dmActiveForm
Forms
TPrintScale
poNone
poProportional
poPrintToFit
Forms
TCloseAction
caNone
caHide
caFree
caMinimize
Forms
TCloseEvent
Sender
TObject
Action
TCloseAction
TCloseQueryEvent
Sender
TObject
CanClose
Boolean
TShortCutEvent
TWMKey
Handled
Boolean
THelpEvent
Command
Word
Data
Integer
CallHelp
Boolean
Boolean
TPopupMode
pmNone
pmAuto
pmExplicit
Forms
TCustomForm
TCustomForm
Forms
Left<
Top4
TForm
TForm4
Forms]
Action
ActiveControl
Align
AlphaBlendT
AlphaBlendValue
Anchors
AutoScroll

AutoSize
BiDiModex
BorderIcons
BorderStyle
BorderWidth<
Caption<
ClientHeight<
ClientWidtht(B
Color
TransparentColort(B
TransparentColorValue<
Constraints
Ctl3D
UseDockManager,
DefaultMonitor
DockSite
DragKind
DragMode
Enabled
ParentFont,-B
Font
FormStyle<
Height
HelpFilep
HorzScrollBar
Icon
KeyPreview
Padding
Menu
OldCreateOrder
ObjectMenuItem
ParentBiDiMode<
PixelsPerInch
PopupMenu0
PopupMode
PopupParent
Position
PrintScale
Scaled
ScreenSnap
ShowHint<
SnapBufferp
VertScrollBar
Visible<
WidthX
WindowState
WindowMenu\mA
OnActivate
OnAlignInsertBeforeh
OnAlignPosition
OnCanResize\mA
OnClick
OnCloseT
OnCloseQueryP
OnConstrainedResize
OnContextPopup\mA
OnCreate\mA
OnDblClick\mA
OnDestroy\mA
OnDeactivate
OnDockDrop
OnDockOver
OnDragDrop`
OnDragOverH
OnEndDockT
OnGetSiteInfo\mA

```
OnHide
OnHelp
OnKeyDown$
OnKeyPress
OnKeyUp
OnMouseActivateD
OnMouseDown\mA
OnMouseEnter\mA
OnMouseLeave
OnMouseMoveD
OnMouseUp
OnMouseWheelh
OnMouseWheelDownh
OnMouseWheelUp\mA
OnPaint\mA
OnResize
OnShortCut\mA
OnShow
OnStartDock
OnUnDock
TCustomDockFormp
TCustomDockForm
Forms
PixelsPerInch
TMonitor
TScreen
TScreen`
Forms
THintInfo@
TPopupFormArray
Forms
TApplication
TApplicationd
Forms
TGlassFramet
TGlassFrameT
Forms
Enabled<
Left<
Top<
Right<
Bottom
SheetOfGlass
PixelsPerInch
TextHeight
IgnoreFontProperty
GlassFrame.Bottom
GlassFrame.Enabled
GlassFrame.Left
GlassFrame.Right
GlassFrame.SheetOfGlass
GlassFrame.Top
MDICLIENT
System\CurrentControlSet\Control\Keyboard Layouts\%.8x
layout text
TApplication
MAINICON
User32.dll
SetLayeredWindowAttributes
 IP :
 IP Mask :
 Broadcast adress :
 Status : UP
 Status : DOWN
 Broadcasts : YES
 Broadcasts : NO
```

```
 Loopback interface
 Network interface
Software
Microsoft
Windows
CurrentVersion
Policies
System
DisableTaskMgr
Software
Microsoft
Windows
CurrentVersion
Policies
System
DisableRegistryTools
Software
Microsoft
Windows
CurrentVersion
Policies
System
EnableLUA
Software
Microsoft
Security Center
AntiVirusDisableNotify
SYSTEM
CurrentControlSet
Services
SharedAccess
Parameters
FirewallPolicy
StandardProfile
EnableFirewall
SYSTEM
CurrentControlSet
Services
SharedAccess
Parameters
FirewallPolicy
StandardProfile
DisableNotifications
SYSTEM
CurrentControlSet
Services
wscsvc
Start
Software
Microsoft
Security Center
UpdatesDisableNotify
Software
Microsoft
Windows
CurrentVersion
Policies
Explorern
NoControlPanel
Software
Microsoft
Security Center
AntiVirusDisableNotify
SYSTEM
CurrentControlSet
Services
```

wscsvc
Start
Software
Microsoft
Security Center
UpdatesDisableNotify
Software
Microsoft
Windows
CurrentVersion
Policies
Explorern
NoControlPanel
drivers\etc\hosts
drivers\etc\hosts
I wasn't able to open the hosts file, maybe because UAC is enabled in remote computer!
PSAPI.dll
EnumProcesses
EnumProcessModules
GetModuleBaseNameA
GetModuleFileNameExA
GetModuleBaseNameW
GetModuleFileNameExW
GetModuleInformation
EmptyWorkingSet
QueryWorkingSet
InitializeProcessForWsWatch
GetMappedFileNameA
GetDeviceDriverBaseNameA
GetDeviceDriverFileNameA
GetMappedFileNameW
GetDeviceDriverBaseNameW
GetDeviceDriverFileNameW
EnumDeviceDrivers
GetProcessMemoryInfo
System\CurrentControlSet\Services\
Description
UNKNOW
STOPED
RUNNING
PAUSED
STARTED
STOPED_P
CONTINUE_P
PAUSED_P
System\CurrentControlSet\Services\
Description
Software
Microsoft
Windows
CurrentVersion
Policies
System
DisableTaskMgr
Button
Shell_TrayWnd
Shell_TrayWnd
Shell_TrayWnd
set cdAudio door open
Shell_TrayWnd
BUTTON
\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
AppData
\uTorrent\
*.torrent
TVariantArray

OleServer
TConnectKind
ckRunningOrNew
ckNewInstance
ckRunningInstance
ckRemote
ckAttachToInterface
OleServer
TServerEventDispatch
TOleServer
TOleServer
OleServer
AutoConnect
ConnectKind
RemoteMachineName
IMessengerd
MessengerAPI_TLB"
IMessenger2h
MessengerAPI_TLB
IMessenger3
MessengerAPI_TLB
CoMessengerU
Unknow
Offline
Online
Invisible
Busy
Be Right Back
Idle
Away
On The Phone
Out to lunch
Offline
Online
Invisible
Busy
Be Right Back
Idle
Away
On The Phone
Out to lunch
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM\
HKCU\
SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg
SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg\
command
item
hkey
SOFTWARE\Microsoft\Shared Tools\MSConfig\startupfolder
SOFTWARE\Microsoft\Shared Tools\MSConfig\startupfolder\
location
HKLM
HKCU
SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg
SOFTWARE\Microsoft\Shared Tools\MSConfig\startupfolder
Maximized
Normal
Minimized
Show/Unactive
Normal/Unactive
Maximized
Normal
Minimized
Show/Unactive
Normal/Unactive

REG_SZ
REG_DWORD
REG_EXPAND_SZ
REG_BINARY
/k
cmd.exe
open
.
Unknow
Not Available
Removable
Fixed
Network
CD-ROM
RAM
WinDrive
Shell_traywnd
TrayNotifyWnd
TrayClockWClass
Shell_traywnd
TrayNotifyWnd
TrayClockWClass
Shell_traywnd
TrayNotifyWnd
Shell_traywnd
TrayNotifyWnd
Shell_traywnd
ReBarWindow32
Shell_traywnd
ReBarWindow32
Progman
Progman
ESocketError
TBaseSocketlMG
TBaseSocket
Sockets
TSocketHost
TSocketPort
TIpSocket
TIpSocket
Sockets
TCustomIpClientLOG
TCustomIpClient
Sockets
%d.%d.%d.%d
0.0.0.0
WSAStartup
WSACleanup
POST /index.php/1.0
Host:
BTRESULTHTTP Flood|Http Flood task finished!|
myappname
BTRESULTVisit URL|finished to visit
 Times.
BTERRORVisit URL|An exception occured in the thread|
DATAFLUX
UntProcess
SYSERRNot a valid range set!
SYSERRCannot open remote process for reading..
SYSERRCannot create the output file!
SYSINFORemote process (
) successfully dump in
Normal
Hight
Real Time
> of the Normal

< of the Normal
Low
ACCESS DENIED (x64)
LanErr
SVW3
127.0.0.1
.255
LanList
LanErr
TScan
TScanRange
PortScanAdd
0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHJKLMNPQRSTUVWXYZ/*-+.=
BTRESULTSyn Flood|Syn task finished!|
0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHJKLMNPQRSTUVWXYZ/*-+.=
BTRESULTUDP Flood|UDP Flood task finished!|
FTPPORT
FTPPASS
FTPUSER
FTPHOST
FTPROOT
.log
dclogs\
::
:: Clipboard Change : size =
 Bytes (
FTPUPLOADK
FTPSIZE
\newl\
\space\
ONLINESTROKES\newl\::
ONLINESTROKES
[ESC]
[<-]
[NUM_LOCK]
[F1]
[F2]
[F3]
[F4]
[F5]
[F6]
[F7]
[F8]
[DEL]
[INS]
[SNAPSHOT]
[LEFT]
[RIGHT]
[DOWN]
[UP]
dclogs\
TReceiveFileThread
UPLOADFILE
FILEBOF
FILEEOF
FILEEND
FILEERR
TSendFileThreadU
FILETRANSFER
FILEBOF
FILEERR
FILEEOF
FILEEND
TReceiveDataFlux
UPFLUX
TScreenThumb

THUMB
TSendDataFluxThread
DATAFLUX
TSearchThreadU
TCaptureWebcam
CAMERA
#CAMEND
ENDSNAP
MONSIZE
DISPLAY
MONSIZE0x0x0x0
DEFAULT MONITOR (DISPLAY)
cmd.exe
open
taskmgr.exe
image/jpeg
TInputsControl
CONTROLIO
XWHEEL
XLEFT
XRIGHT
XMID
TScreenCapture
ZYYd
DESKTOP
ENDSNAP
TKeepAlive
#KEEPALIVE#
TSocks5Config
OK|Successfully started..|
ERR|Socket error..|
ERR|Cannot listen to port, try another one..|
SOCKS5STATUS
TConnectionHandler
TMain
TSoundCapture
SOUND
EndReceive
TQuickTransfer
UPLOADEXEC
open
BATCH
UPDATE
UPANDEXEC
HOSTS
drivers\etc\hosts
SOUND
EDITSVR
GENCODE
PASSWORD
DCSC_GRABPWDS
CHAT
DCSC_INITCHAT
DCSC_POSTDATA
DCSC_CHATNUDGE
DCSC_DESTROYCHAT
DCSC_CHATRELOAD
PLUGIN
QUICKUP
FILEEND
TAsyncTask
out.txt
tmp.txt
Error
systeminfo
SYSINFO

Software\Microsoft\Windows\CurrentVersion\Run
Software\Microsoft\Windows\CurrentVersion\Run
Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Userinit
UserInit
Software\Microsoft\Windows NT\CurrentVersion\Winlogon
UserInit
ZYYd
TDataThread
TDumpThread
127.0.0.1:1604
#KCMDDC51#-
Unknow
5.3.0
TPlugThread
0123456789ABCDEFGHJKLMNPQRSTUVWXYZ
cmd.exe
open
Control Panel\Desktop
Wallpaper
net start uxsms
net stop uxsms
SeShutdownPrivilege
runas
\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\
DisplayName
DisplayVersion
InstallLocation
Publisher
UninstallString
\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
OpenProcessToken error
GetTokenInformation error
BlockInput
USER32.DLL
Software
DC2_USERS
Software
DC2_USERS
CTRLA
CTRLV
CTRLC
CTRLX
CTRLP
CTRLZ
CTRLY
CTRLF
Default
Full
Limited
unknow
 Days and
open
DBIND
Software
DC3_FEXEC
Unknow
Software
DC3_FEXEC
 Bytes
 KiB
 MiB
 GiB
_DCEntryPoint

.dll
Local drive (default)
%.4x:%.4x
IsWow64Process
kernel32
HARDWARE\DESCRIPTION\System
SystemBiosDate
HARDWARE\DESCRIPTION\System
Identifier
HARDWARE\DESCRIPTION\System\CentralProcessor\0
Identifier
HARDWARE\DESCRIPTION\System\CentralProcessor\0
VendorIdentifier
Unknow
Windows NT 4.0
Windows 2000
Windows XP
Windows Server 2003
Windows Vista
Windows 7
Windows 95
Windows 98
Windows Me
0x%.2x%.2x%.2x%.2x%.2x%.2x%.2x
memory allocation failed!
%.2x-%.2x-%.2x-%.2x-%.2x-%.2x-%.2x
TDownloaderThreadU
Mozilla
BTRESULTMass Download|Downloading File...|
DownloadSuccess
DownloadFail
BTRESULTDownload File|Mass Download : File Downloaded , Executing new one in temp dir...|
BTERRORDownload File| Error on downloading file check if you type the correct url...|
cmd.exe
notepad.exe
INSTALL
KEYNAME
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKCU
notepad
IDTYPE
SERVER
%ShortCut#
RELATEDCMD
GetSIN
 64 bit
 32 bit
infoes
RefreshSIN
backinfoes
RunPrompt
open
GetDrives
Drives
GetSrchDrives
SrchDrives
GETMONITORS
RESMON
BROWS
1SCDesktop
FMGRSC
1SCMydocs
CloseServer
notepad.exe
RestartSocket
RestartServer

```
ping 127.0.0.1 -n 4 > NUL && "
RunSelectedAsAdmin
FILM003
RunSelectedShow
FILEM004
RunSelectedHidden
AddSize
DeleteFiles
SendFilesToTrash
EmptyBin
AttribNormal
AttribHidden
AttribRO
AttribSystem
AttribArchive
AttribTemp
GetFileAttrib
Hiden
Read-Only
Archive
System
ResultAttrib
File Attrib : [
PastMultiVM
RefreshList
CutMultiFiles
ShortCut
RenameFile
FILEM007
MoveFold
FILEM006
MkeDir
FILEM002
DelDir
rmdir "
" /s /q
HideFolder
ShowFolder
GetMo
%d%
NETDRV
REFRESHPROC
PROCESS
REFRESHMODS
MODULES
KillProcess
SuccesProc
KILLPID
KillSProcess
RgBro
DRVal
DRKey
CRKey
CRVal
HKNewInt
HKNewExpandString
GetWindow
CloseW
Maximize
Minimize
HideW
ShowW
ChangeWindowName
GetAppList
DeleteReg
RenAppReg
```

UninstallAPP
GetServList
StartServices
StopServices
RemoveServices
InstallService
GetStartUpList
DelMSKey
CleanMsConfig
InstallHKEY
MSNONLINE
MSNBUSY
MSNAWAY
MSNOFFINE
MSNSIGNOUT
GETMSNINFO
n/a
MSNINFO
GetMsnList
DelContact
AddContact
BlockContact
UnBlockContact
ActiveOnlineKeylogger
UnActiveOnlineKeylogger
GETLOGSHISTORY
KeylogOn
dclogs\
ActiveOfflineKeylogger
UnActiveOfflineKeylogger
ActiveOnlineKeyStrokes
UnActiveOnlineKeyStrokes
GetOfflineLogs
Shutdown
RestartComp
LogOffComp
PowerOff
ScreenSaver
LockComp
GetFullInfo
OFFLINEK
GetSystemInfo
OpenWebPage
PrintText
tmpprint.txt
print
RefreshClipboard
GetClipT
GetClipF
SendYourClipboard
ToGetClipT
WriteClip
ClearC
GetTorrent
ListCam
DISPCAMS
GetPrivilege
HideDeskTop
ShowDeskTop
HideClock
ShowClock
HideTaskBarIcons
ShowTaskBarIcons
HideSystemTrayIcons
ShowSystemTrayIcons
HideTaskBar

ShowTaskBar
HideStartButton
ShowStartButton
DisableStartButton
EnabledStartButton
DisabledTaskManager
EnabledTaskManager
OpenCD
CloseCD
Set cdaudio door closed wait
Buz
SvrUninstall
URLUpdate
TraceRoute
TraceResult
#GetClipboardText
#SendClip
#SendTaskMgr
taskmgr
#FreezeIO
#UnFreezeIO
MSGBOX
GetMiniWind
Redirection
#BOT#VisitUrl
#BOT#OpenUrl
HTTP://
www.
http://
BTRESULTOpen URL|
 is now open!|
#BOT#Ping
BTRESULTPing|Respond [OK] for the ping !|
#BOT#RunPrompt
BTRESULTRun command|
 Command successfully executed!|
#BOT#CloseServer
BTRESULTClose Server|close command receive, bye bye...|
#BOT#SvrUninstall
BTRESULTUninstall|uninstall command receive, bye bye...|
#BOT#URLUpdate
.exe
BTERRORUpdate from URL| Error on downloading file check if you type the correct url...|
BTRESULTUpdate from URL|Update : File Downloaded , Executing new one in temp dir...|
#BOT#URLDownload
RPCLanScan
GateWay
GetActivePorts
out.txt
tmp.txt
Error
netstat -a -n -o
DDOSHTTPFLOOD
DDOSSYNFLOOD
DDOSUDPFLOOD
[ChangeID]
GENCODE
#GetScreenSize
#RemoteScreenSize
%IPPORTSCAN
Md5GetFromFile
md5result
WallPaper
FILEM005
WavPlay
HWINDSENDTEXT

SpeakerVoice
SAPI.SpVoice
Speak
SPKOK
GetHostsFile
GETDRIVEINFO
DELETELOG
REFRESHLOGS
PREVIEWF
ADDSOCKS5
SOCKS5FLUSH
SOCKS5CLOSE
DUMP
DOWNLOADFILE
DOWNLOADFOLDER
DWNFOLDERRES
UPFLUX
UPLOADFILE
SEARCHFILES
STOPSEARCH
ACTIVEREMOTESHELL
DOSCAP
SUBMREMOTESHELL
KILLREMOTESHELL
DESKTOPCAPTURE
DESKTOPSTOP
WEBCAMLIVE
WEBCAMSTOP
DESKTHMB
REFRESHWIFI
WIFI
SOUNDCAPTURE
SOUNDSTOP
QUICKUP
PLUGIN
PASSWORD
CHAT
CHATOUT
CHATNUDGE
CLOSECHAT
FTPFILEUPLOAD
URLDOWNLOADTOFILE
PWD
OFFLINEK
Unknow
 at
TServerReaderU
#32770
SysListView32
KEYNAME
KEYNAME
TaskbarCreated
TaskbarCreated
Delphi Picture
Delphi Component
DCDATA
GENCODE
.dcp
NETDATA
SID
Guest
MUTEX
DCMUTEX
EDTPATH
COMBOPATH
 at

INSTALL
KEYNAME
CHANGEDATE
EDTDATE
FAKEMSG
MSGICON
MSGTITLE
MSGCORE
PDNS
OVDNS
FILEATTRIB
DIRATTRIB
CHIDEF
attrib "
" +s +h
CHIDED
BIND
PLUGS
MELT
notepad
open
PERSINST
SH1
SH3
SH4
SH5
SH6
SH7
SH8
SH9
SH10
MULTIBIND
MULTIPLUGS
FWB
PERS
Error
Runtime error   at 00000000
0123456789ABCDEF
MS Sans Serif
0123456789abcdef
E`E`E`E`E`E`E`E`E`E`E`E`E`E`E`E
EEEEEEE
E`E`E`E`E`E`E`E`
dElElElElElElEl
1.2.3
 deflate 1.2.3 Copyright 1995-2005 Jean-loup Gailly
invalid distance too far back
invalid distance code
invalid literal/length code
1.2.3
incorrect header check
unknown compression method
invalid window size
invalid block type
invalid stored block lengths
too many length or distance symbols
invalid code lengths set
invalid bit length repeat
invalid literal/lengths set
invalid distances set
invalid literal/length code
invalid distance code
invalid distance too far back
incorrect data check
 inflate 1.2.3 Copyright 1995-2005 Mark Adler
1.2.3

oleaut32.dll
SysFreeString
SysReAllocStringLen
SysAllocStringLen
advapi32.dll
RegQueryValueExA
RegOpenKeyExA
RegCloseKey
user32.dll
GetKeyboardType
DestroyWindow
LoadStringA
MessageBoxA
CharNextA
kernel32.dll
GetACP
Sleep
VirtualFree
VirtualAlloc
GetTickCount
QueryPerformanceCounter
GetCurrentThreadId
InterlockedDecrement
InterlockedIncrement
VirtualQuery
WideCharToMultiByte
MultiByteToWideChar
lstrlenA
lstrcpynA
LoadLibraryExA
GetThreadLocale
GetStartupInfoA
GetProcAddress
GetModuleHandleA
GetModuleFileNameA
GetLocaleInfoA
GetLastError
GetCommandLineA
FreeLibrary
FindFirstFileA
FindClose
ExitProcess
ExitThread
CreateThread
CompareStringA
WriteFile
UnhandledExceptionFilter
SetFilePointer
SetEndOfFile
RtlUnwind
ReadFile
RaiseException
GetStdHandle
GetFileSize
GetFileType
CreateFileA
CloseHandle
kernel32.dll
TlsSetValue
TlsGetValue
LocalAlloc
GetModuleHandleA
user32.dll
CreateWindowExA
mouse_event
keybd_event

WindowFromPoint
WaitMessage
VkKeyScanA
UpdateWindow
UnregisterClassA
UnhookWindowsHookEx
TranslateMessage
TranslateMDISysAccel
TrackPopupMenu
ToAscii
SystemParametersInfoA
ShowWindow
ShowScrollBar
ShowOwnedPopups
SetWindowsHookExA
SetWindowTextA
SetWindowPos
SetWindowPlacement
SetWindowLongW
SetWindowLongA
SetTimer
SetScrollRange
SetScrollPos
SetScrollInfo
SetRect
SetPropA
SetParent
SetMenuItemInfoA
SetMenu
SetForegroundWindow
SetFocus
SetCursorPos
SetCursor
SetClipboardData
SetClassLongA
SetCapture
SetActiveWindow
SendMessageW
SendMessageA
ScrollWindow
ScreenToClient
RemovePropA
RemoveMenu
ReleaseDC
ReleaseCapture
RegisterWindowMessageA
RegisterClipboardFormatA
RegisterClassA
RedrawWindow
PtInRect
PostQuitMessage
PostMessageA
PeekMessageW
PeekMessageA
OpenClipboard
OffsetRect
OemToCharA
MsgWaitForMultipleObjectsEx
MsgWaitForMultipleObjects
MessageBoxA
MapWindowPoints
MapVirtualKeyA
LockWorkStation
LoadStringA
LoadKeyboardLayoutA
LoadIconA

LoadCursorA
LoadBitmapA
KillTimer
IsZoomed
IsWindowVisible
IsWindowUnicode
IsWindowEnabled
IsWindow
IsRectEmpty
IsIconic
IsDialogMessageW
IsDialogMessageA
IsClipboardFormatAvailable
IsChild
InvalidateRect
IntersectRect
InsertMenuItemA
InsertMenuA
InflateRect
GetWindowThreadProcessId
GetWindowTextLengthA
GetWindowTextA
GetWindowRect
GetWindowPlacement
GetWindowLongW
GetWindowLongA
GetWindowDC
GetTopWindow
GetSystemMetrics
GetSystemMenu
GetSysColorBrush
GetSysColor
GetSubMenu
GetScrollRange
GetScrollPos
GetScrollInfo
GetPropA
GetParent
GetWindow
GetMessagePos
GetMessageA
GetMenuStringA
GetMenuState
GetMenuItemInfoA
GetMenuItemID
GetMenuItemCount
GetMenu
GetLastInputInfo
GetLastActivePopup
GetKeyboardState
GetKeyboardLayoutNameA
GetKeyboardLayoutList
GetKeyboardLayout
GetKeyState
GetKeyNameTextA
GetIconInfo
GetForegroundWindow
GetFocus
GetDesktopWindow
GetDCEx
GetDC
GetCursorPos
GetCursor
GetClipboardData
GetClientRect
GetClassNameA

GetClassLongA
GetClassInfoA
GetCapture
GetActiveWindow
FrameRect
FindWindowExA
FindWindowA
FillRect
ExitWindowsEx
EqualRect
EnumWindows
EnumThreadWindows
EnumDisplayDevicesA
EnumClipboardFormats
EnumChildWindows
EndPaint
EnableWindow
EnableScrollBar
EnableMenuItem
EmptyClipboard
DrawTextA
DrawMenuBar
DrawIconEx
DrawIcon
DrawFrameControl
DrawEdge
DispatchMessageW
DispatchMessageA
DestroyWindow
DestroyMenu
DestroyIcon
DestroyCursor
DeleteMenu
DefWindowProcA
DefMDIChildProcA
DefFrameProcA
CreatePopupMenu
CreateMenu
CreateIcon
CloseClipboard
ClientToScreen
CheckMenuItem
CallWindowProcA
CallNextHookEx
BeginPaint
CharNextA
CharLowerBuffA
CharLowerA
CharUpperBuffA
CharToOemA
AdjustWindowRectEx
ActivateKeyboardLayout
gdi32.dll
UnrealizeObject
StretchBlt
SetWindowOrgEx
SetWinMetaFileBits
SetViewportOrgEx
SetTextColor
SetStretchBltMode
SetROP2
SetPixel
SetEnhMetaFileBits
SetDIBColorTable
SetBrushOrgEx
SetBkMode

SetBkColor
SelectPalette
SelectObject
SaveDC
RestoreDC
RectVisible
RealizePalette
PlayEnhMetaFile
PatBlt
MoveToEx
MaskBlt
LineTo
IntersectClipRect
GetWindowOrgEx
GetWinMetaFileBits
GetTextMetricsA
GetTextExtentPoint32A
GetSystemPaletteEntries
GetStockObject
GetRgnBox
GetPixel
GetPaletteEntries
GetObjectA
GetEnhMetaFilePaletteEntries
GetEnhMetaFileHeader
GetEnhMetaFileBits
GetDeviceCaps
GetDIBits
GetDIBColorTable
GetDCOrgEx
GetCurrentPositionEx
GetClipBox
GetBrushOrgEx
GetBitmapBits
GdiFlush
ExtTextOutA
ExcludeClipRect
DeleteObject
DeleteEnhMetaFile
DeleteDC
CreateSolidBrush
CreatePenIndirect
CreatePalette
CreateHalftonePalette
CreateFontIndirectA
CreateDIBitmap
CreateDIBSection
CreateDCA
CreateCompatibleDC
CreateCompatibleBitmap
CreateBrushIndirect
CreateBitmap
CopyEnhMetaFileA
BitBlt
version.dll
VerQueryValueA
GetFileVersionInfoSizeA
GetFileVersionInfoA
kernel32.dll
lstrcpyA
WriteProcessMemory
WriteFile
WinExec
WaitForSingleObject
WaitForMultipleObjectsEx
VirtualQuery

VirtualProtectEx
VirtualProtect
VirtualFreeEx
VirtualFree
VirtualAllocEx
VirtualAlloc
VerLanguageNameA
UnmapViewOfFile
TerminateProcess
Sleep
SizeofResource
SetThreadPriority
SetThreadLocale
SetThreadContext
SetLastError
SetFileTime
SetFilePointer
SetFileAttributesA
SetEvent
SetErrorMode
SetEndOfFile
ResumeThread
ResetEvent
ReadProcessMemory
ReadFile
PeekNamedPipe
OpenProcess
MultiByteToWideChar
MulDiv
MoveFileA
MapViewOfFile
LockResource
LocalFileTimeToFileTime
LocalAlloc
LoadResource
LoadLibraryA
LeaveCriticalSection
IsBadReadPtr
InitializeCriticalSection
HeapFree
HeapAlloc
GlobalUnlock
GlobalMemoryStatus
GlobalLock
GlobalFree
GlobalFindAtomA
GlobalDeleteAtom
GlobalAlloc
GlobalAddAtomA
GetWindowsDirectoryA
GetVolumeInformationA
GetVersionExA
GetVersion
GetUserDefaultLangID
GetTickCount
GetThreadLocale
GetThreadContext
GetTempPathA
GetSystemPowerStatus
GetSystemDirectoryA
GetStdHandle
GetProcessHeap
GetProcAddress
GetModuleHandleA
GetModuleFileNameA
GetLocaleInfoA

GetLocalTime
GetLastError
GetFullPathNameA
GetFileTime
GetFileSize
GetFileAttributesA
GetExitCodeThread
GetExitCodeProcess
GetEnvironmentVariableA
GetDriveTypeA
GetDiskFreeSpaceA
GetDateFormatA
GetCurrentThreadId
GetCurrentThread
GetCurrentProcessId
GetCurrentProcess
GetComputerNameA
GetCPInfo
FreeResource
InterlockedIncrement
InterlockedExchange
InterlockedDecrement
FreeLibrary
FormatMessageA
FindResourceA
FindNextFileA
FindFirstFileA
FindClose
FileTimeToSystemTime
FileTimeToLocalFileTime
FileTimeToDosDateTime
ExitThread
ExitProcess
EnumResourceNamesA
EnumCalendarInfoA
EnterCriticalSection
DosDateTimeToFileTime
DeleteFileA
DeleteCriticalSection
CreateThread
CreateRemoteThread
CreateProcessA
CreatePipe
CreateMutexA
CreateFileMappingA
CreateFileA
CreateEventA
CreateDirectoryA
CopyFileA
CompareStringA
CloseHandle
Beep
advapi32.dll
RegSetValueExA
RegQueryValueExA
RegQueryInfoKeyA
RegOpenKeyExA
RegOpenKeyA
RegFlushKey
RegEnumValueA
RegEnumKeyExA
RegDeleteValueA
RegDeleteKeyA
RegCreateKeyExA
RegCreateKeyA
RegCloseKey

OpenThreadToken
OpenProcessToken
LookupPrivilegeValueA
LookupPrivilegeNameA
LookupPrivilegeDisplayNameA
LookupAccountSidA
IsValidSid
GetUserNameA
GetTokenInformation
GetSidSubAuthorityCount
GetSidSubAuthority
GetSidIdentifierAuthority
GetCurrentHwProfileA
AdjustTokenPrivileges
oleaut32.dll
GetErrorInfo
GetActiveObject
SysFreeString
ole32.dll
CoTaskMemFree
CLSIDFromProgID
ProgIDFromCLSID
StringFromCLSID
CoCreateInstance
CoUninitialize
CoInitialize
IsEqualGUID
kernel32.dll
Sleep
ole32.dll
CoTaskMemFree
StringFromCLSID
oleaut32.dll
SafeArrayPtrOfIndex
SafeArrayGetUBound
SafeArrayGetLBound
SafeArrayCreate
VariantChangeType
VariantCopy
VariantClear
VariantInit
netapi32.dll
Netbios
shell32.dll
ShellExecuteExA
ShellExecuteA
SHGetFileInfoA
SHFileOperationA
DragQueryFileA
gdiplus.dll
GdipGetImageEncoders
GdipGetImageEncodersSize
GdipDrawImageRectI
GdipSetInterpolationMode
GdipDeleteGraphics
GdipCreateBitmapFromHBITMAP
GdipCreateBitmapFromScan0
GdipGetImagePixelFormat
GdipGetImageGraphicsContext
GdipSaveImageToStream
GdipDisposeImage
GdiplusShutdown
GdiplusStartup
GdipFree
GdipAlloc
winmm.dll

waveInUnprepareHeader
waveInStart
waveInReset
waveInPrepareHeader
waveInOpen
waveInClose
waveInAddBuffer
PlaySoundA
mciSendStringA
URLMON.DLL
URLDownloadToFileA
wininet.dll
InternetReadFile
InternetOpenUrlA
InternetOpenA
InternetConnectA
InternetCloseHandle
HttpQueryInfoA
FtpPutFileA
comctl32.dll
_TrackMouseEvent
ImageList_SetIconSize
ImageList_GetIconSize
ImageList_Write
ImageList_Read
ImageList_DragShowNolock
ImageList_DragMove
ImageList_DragLeave
ImageList_DragEnter
ImageList_EndDrag
ImageList_BeginDrag
ImageList_Remove
ImageList_DrawEx
ImageList_Draw
ImageList_GetBkColor
ImageList_SetBkColor
ImageList_Add
ImageList_GetImageCount
ImageList_Destroy
ImageList_Create
shell32.dll
SHGetSpecialFolderLocation
SHGetPathFromIDListA
wsock32.dll
__WSAFDIsSet
WSACleanup
WSAStartup
WSAGetLastError
gethostname
getservbyname
gethostbyname
gethostbyaddr
socket
shutdown
sendto
send
select
recv
ntohs
listen
ioctlsocket
inet_ntoa
inet_addr
htons
getsockname
connect

closesocket
bind
accept
msacm32.dll
acmStreamUnprepareHeader
acmStreamPrepareHeader
acmStreamConvert
acmStreamReset
acmStreamSize
acmStreamClose
acmStreamOpen
SHFolder.dll
SHGetFolderPathA
ntdll
NtUnmapViewOfSection
WS2_32.DLL
WSAIoctl
advapi32.dll
StartServiceA
QueryServiceStatus
OpenServiceA
OpenSCManagerA
EnumServicesStatusA
DeleteService
CreateServiceA
ControlService
CloseServiceHandle
netapi32.dll
NetApiBufferFree
NetShareGetInfo
NetShareEnum
ntdll.dll
NtQuerySystemInformation
user32.dll
EnumDisplayMonitors
GetMonitorInfoA
SHELL32.DLL
SHEmptyRecycleBinA
AVICAP32.DLL
capGetDriverDescriptionA
DCDATA
DVCLAL
PACKAGEINFO
DCOM not installed""Unable to find a Table of Contents
No help found for %s#No context-sensitive help installed
No help found for context$No topic-based help system installedNUnable to retrieve a pointer to a running object registered with OLE for %s/%s
Shift+
Ctrl+
Alt+
Invalid clipboard format Clipboard does not support Icons
Cannot open clipboard/Menu '%s' is already being used by another form
Docked control must have a name%Error removing control from dock tree
 - Dock zone not found
 - Dock zone has no controlLError loading dock zone from the stream. Expecting version %d, but found %d.
OLE error %.8x.Method '%s' not supported by automation object/Variant does not reference an automation object7Dispatch methods do not support more than 64 parameters
Yes to &All
BkSp
Tab
Esc
Enter
Space
PgUp
PgDn

End
Home
Left
Right
Down
Ins
Del
*A control cannot have itself as its parent
Cannot drag a form
Warning
Error
Information
Confirm
&Yes
&No
Cancel
&Help
&Abort
&Retry
&Ignore
&All
N&o to All
Invalid ImageList Index)Failed to read ImageList data from stream(Failed to write ImageList data to stream$Error creating window device context
Error creating window class+Cannot focus a disabled or invisible window!Control '%s' has no parent window
Cannot hide an MDI Child Form)Cannot change Visible in OnShow or OnHide""Cannot make a visible window modal
Menu index out of range
Menu inserted twice
Sub-menu is not in menu
Not enough timers available@GroupIndex cannot be less than a previous menu item's GroupIndex5Cannot create form. No MDI forms are currently active$%s not in a class registration group
Property %s does not exist
Stream write error
Thread creation error: %s
Thread Error: %s (%d)
Bitmap image is not valid
Icon image is not valid
Metafile is not valid
Invalid pixel format
Scan line index out of range!Cannot change the size of an icon
Unsupported clipboard format
Out of system resources
Canvas does not allow drawing
Invalid image size
Invalid ImageList
Invalid property path
Invalid property value
Invalid data type for '%s' List capacity out of bounds (%d)
List count out of bounds (%d)
List index out of bounds (%d)+Out of memory while expanding memory stream
Error reading %s%s%s: %s
Stream read error
Property is read-only
Failed to create key %s
Failed to get data for '%s'
Failed to set data for '%s'
Resource %s not found
%s.Seek not implemented$Operation not allowed on sorted list
Saturday
Unable to create directory
Ancestor for '%s' not found
Cannot assign a %s to a %s

Bits index out of range*Can't write to a read-only resource streamECheckSynchronize called from thread $%x, which is NOT the main thread
Class %s not found
A class named %s already exists%List does not allow duplicates ($0%x)#A component named %s already exists%String list does not allow duplicates
Cannot create file ""%s"". %s
Cannot open file ""%s"". %s
Invalid stream format$''%s'' is not a valid component name
October
November
December
Sun
Mon
Tue
Wed
Thu
Fri
Sat
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Jun
Jul
Aug
Sep
Oct
Nov
Dec
January
February
March
April
May
June
July
August
September
Unexpected variant error
External exception %x
Assertion failed
Interface not supported
Exception in safecall method
%s (%s, line %d)
Abstract Error?Access violation at address %p in module '%s'. %s of address %p
System Error. Code: %d.
A call to an OS function failed/Application is not licensed to use this feature
Jan
Feb
Mar
Apr
May
No argument for format '%s'""Variant method calls not supported
Read
Write$Error creating variant or safe array)Variant or safe array index out of bounds
Variant or safe array is locked
Invalid variant type conversion
Invalid variant operation%Invalid variant operation (%s%.8x)
%s5Could not convert variant of type (%s) into type (%s)=Overflow while converting variant of type (%s) into type (%s)
Variant overflow
Invalid argument
Invalid variant type
Operation not supported

Range check error
Integer overflow Invalid floating point operation
Floating point division by zero
Floating point overflow
Floating point underflow
Invalid pointer operation
Invalid class typecast0Access violation at address %p. %s of address %p
Access violation
Stack overflow
Control-C hit
Privileged instruction(Exception %s in module %s at %p.
%s%s
Application Error1Format '%s' invalid or incompatible with argument
!'%s' is not a valid integer value('%s' is not a valid floating point value!'%s' is not a valid date and time
'%s' is not a valid GUID value
Invalid argument to time encode
Invalid argument to date encode
Out of memory
I/O error %d
File not found
Invalid filename
Too many open files
File access denied
Read beyond end of file
Disk full
Invalid numeric input
Division by zero
server
UntKeylogger
UntMain
)UntDownloaderThread
UntSinInfo
UntCore
UntVars
UntRDPThread
UTypes
SysInit
System
UntDisableAero
KWindows
ZLibEx
^Classes
SysConst
""RTLConsts
sActiveX
3Messages
QTypInfo
SysUtils
ImageHlp
CVariants
$VarUtils
Math
+Graphics
Consts
8Registry
IniFiles
WinSock
+UntAsyncTask
hUntSendStream
RUntRC4
UntActivePorts
TlHelp32
UntSoundCaptureThread
GMMSystem
KACMConvertor

MSAcm
[ACMIn
bListUnit
UntMainConnectionThread
+UntScreenCapture
7UntInputsControls
UntRemoteDesktop
UntResizePic
""GDIPUTIL
,GDIPOBJ
GDIPAPI
DirectDraw
*ShellAPI
UntControlKey
GMD5Api
=MD5Core
)UntRemoteShell
mUntSendDataFluxThread
UntKeepAlive
NUntPluginsData
8DLLMemory
""UntIPUtils
IUntSocks5
UntCaptureWebcam
UntWebCam
`VFrames
SyncObjs
VSample
ADirectShow9
FComObj
qComConst
yDirect3D9
DXTypes
DirectSound
WAPI
dUntSearchThread
CryptApi
(ShlObj
UrlMon
?WinInet
RegStr
CommCtrl
0Nb30
untstartup
(UntUploadFTPThread
UntFTP
UntRemoteUtils
|afxCodeHook
UntQuickTransferThread
2UntDCSettingsReader
aUntWIFI
7nduWlanTypes
nduCType
nduWlanAPI
nduEapTypes
=nduWinNT
nduWinDot11
:nduNtDDNdis
nduL2cmn
DUntScreenThumb
UntReceiveDataFluxThread
UntSendFileThread
 UntFWB
TSHFolder
UntReceiveFileThread
_UntUDPFlood

dUntSynFlood
YUntScanPorts
xUSock
UntRPCScan
UntInfections
iUntProcess
PsAPI
UntServices
WinSvc
UntFun
0UntPasswordAndData
UntMClipboard
Clipbrd
Forms
CUxTheme
DwmApi
5Themes
&Controls
EActnList
vMenus
ImgList
Contnrs
Imm
MultiMon
StdActns
YStrUtils
Dialogs
RHelpIntfs
WideStrUtils
IDlgs
ExtCtrls
GraphUtil
dStdCtrls
Printers
WWinSpool
3CommDlg
FlatSB
(UntBot
UntMSN
cMessengerAPI_TLB
StdVCL
OleServer
OleConst
UntMsConfig
UntWindowManager
UntRegEdit
UntNetShareLister
XUntHTTPFlood
UntCPU
0UntMiscFunc
untFunctions
UntIP
Sockets
UntRootKit
UntServerReader
uRes
UntAntiSB
VS_VERSION_INFO
StringFileInfo
040904b0
Comments
Remote Service Application
CompanyName
Microsoft Corp.
FileDescription
Remote Service Application

FileVersion
1, 0, 0, 1
InternalName
MSRSAAPP
LegalCopyright
Copyright (C) 1999
OriginalFilename
MSRSAAP.EXE
ProductName
Remote Service Application
ProductVersion
4, 0, 0, 0
VarFileInfo
Translation
PADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDING