Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 174, Task ID: 695

Task ID: 695 Risk Level:

Date Processed: 2016-04-28 13:06:31 (UTC)

Processing Time: 61.08 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\c15f543da83b0ca8766e750f61a8b0f7.exe"

Sample ID: Type: basic admin Owner:

c15f543da83b0ca8766e750f61a8b0f7 Label:

2016-04-28 12:45:08 (UTC) Date Added: PE32:win32:gui File Type:

File Size: 692224 bytes

c15f543da83b0ca8766e750f61a8b0f7 MD5:

e40bf835e832252ce631ad2da6fe179d3bca874503496541ca7dda21e894371d SHA256:

Description: None

Pattern Matching Results

5 Packer: Asprotect 2 PE: Nonstandard section

5 PE: Contains compressed section

Static Events

Anomaly: PE: Contains a virtual section

Anomaly: PE: Contains one or more non-standard sections

ASProtect Packer:

Process/Thread Events

Creates process: C:\WINDOWS\Temp\c15f543da83b0ca8766e750f61a8b0f7.exe

["c:\windows\temp\c15f543da83b0ca8766e750f61a8b0f7.exe"]

Named Object Events

Creates mutex: \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex:

\BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-Creates mutex:

507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex: \BaseNamedObjects\MutexNPA_UnitVersioning_1300 \BaseNamedObjects\MSCTF.Shared.MUTEX.MK Creates mutex:

\BaseNamedObjects\userenv: User Profile setup event Creates event:

Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D} Creates semaphore:

File System Events

C:\WINDOWS\Prefetch\C15F543DA83B0CA8766E750F61A8B-001FFFE2.pf Opens:

Opens: C:\Documents and Settings\Admin Opens: C:\WINDOWS\system32\hhctrl.ocx Opens: C:\WINDOWS\system32\imm32.dll Opens: C:\WINDOWS\system32\comctl32.dll

Opens: C:\WINDOWS\system32\comctl32.dll.124.Manifest Opens: C:\WINDOWS\system32\comctl32.dll.124.Config

Opens: C:\WINDOWS\system32\shell32.dll

Opens: C:\WINDOWS\system32\shell32.dll.124.Manifest Opens: C:\WINDOWS\system32\shell32.dll.124.Config C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-

Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83

C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Opens:

Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll

C:\WINDOWS\WindowsShell.Manifest Opens: C:\WINDOWS\WindowsShell.Config Opens: C:\WINDOWS\system32\wsock32.dll Opens: C:\WINDOWS\system32\ws2_32.dll Opens: Opens: C:\WINDOWS\system32\ws2help.dll

C:\WINDOWS\Temp\c15f543da83b0ca8766e750f61a8b0f7.exe Opens:

Opens: C:\

C:\WINDOWS\system32\MSCTF.dll Opens:

C:\WINDOWS\system32\MSCTFIME.IME Opens: C:\WINDOWS\system32\wship6.dll Opens: Opens: C:\WINDOWS\system32\rpcss.dll C:\WINDOWS\system32\uxtheme.dll Opens: Opens: C:\WINDOWS\Fonts\sserife.fon

Windows Registry Events

Creates key:

Creates key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}$

folders

Creates kev: HKCU\software\microsoft\windows\currentversion\explorer\shell folders Creates key: HKLM\software\microsoft\windows\currentversion\explorer\user shell

folders

Creates key: HKLM\software\microsoft\windows\currentversion\explorer\shell folders

Creates kev: HKCU\software\recovery toolbox for rar

HKCU\software\recovery toolbox for rar\cbfilename Creates key: $\label{lem:hkcu} \mbox{HKCU\software\recovery toolbox for rar\cbunzipfolder} \label{lem:hkcu}$ Creates kev:

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\c15f543da83b0ca8766e750f61a8b0f7.exe

Opens key: HKLM\system\currentcontrolset\control\terminal server Opens key: HKLM\system\currentcontrolset\control\safeboot\option

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\secur32.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\rpcrt4.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\advapi32.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon

HKLM\ Opens key:

Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\user32.dll

Opens kev: HKLM\system\currentcontrolset\control\session manager

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\imm32.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\ntdll.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\kernel32.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\gdi32.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msvcrt.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\ole32.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\oleaut32.dll

Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\version.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\comctl32.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\shlwapi.dll

Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\shell32.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\comdlg32.dll

HKLM\software\microsoft\windows nt\currentversion\image file execution

Opens key: options\hhctrl.ocx

Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\system\currentcontrolset\control\error message instrument Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ compatibility 32$ Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

Opens key: HKLM\software\microsoft\windows nt\currentversion\windows

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

Opens key: HKCR\interface\{00020400-0000-0000-c000-00000000046}

HKLM\software\microsoft\oleaut Opens key: HKLM\software\microsoft\oleaut\userera Opens key:

Opens key: HKCU\

Opens key: HKCU\software\policies\microsoft\control panel\desktop

Opens key: HKCU\control panel\desktop

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance

Opens key: HKLM\system\setup

Opens key:

HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots

Opens key: $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+ advanced | \\$ Opens key: $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + nt + current + version + language pack$

Opens key: HKLM\software\microsoft\rpc\pagedbuffers Opens key: HKLM\software\microsoft\rpc

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

 $options \verb|\c15f543da83b0ca8766e750f61a8b0f7.exe \verb|\c15f543da83b0ca8766e750f7.exe \verb|\c15$ Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\svstem\currentcontrolset\control\computername

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername

Opens key: HKLM\software\microsoft\internet explorer

HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key:

options\ws2help.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\ws2_32.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\wsock32.dll

Opens key: HKCU\software\borland\locales Opens key: HKCU\software\borland\delphi\locales

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005

Opens kev:

Opens kev:

Opens key:

Opens key:

Opens kev:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5

Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001

Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003

HKCU\software\recovery toolbox for rar Opens key: HKLM\software\recovery toolbox for rar Opens key:

HKCU\software\classes\ Opens key: Opens key: HKCU\software\classes\.key Opens key: HKLM\software\classes

Opens key: HKCR\.key

Opens key: HKLM\software\borland\locales

Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msctf.dll

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus ctf \setminus compatibility \setminus c15f543 da83b0 ca8766e750f61a8b0f7.exe$

Opens key: HKLM\software\microsoft\ctf\systemshared\

HKCU\keyboard layout\toggle Opens kev: Opens key: HKLM\software\microsoft\ctf\

Opens key: HKLM\software\microsoft\windows nt\currentversion\imm

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\lavers Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msctfime.ime

Opens kev: HKCU\software\microsoft\ctf

Opens key: HKLM\software\microsoft\ctf\systemshared

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\wship6.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\userenv.dll

HKLM\system\currentcontrolset\control\productoptions Opens key:

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders

Opens key: HKLM\software\policies\microsoft\windows\system

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

1757981266-507921405-1957994488-1003

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist

Opens key: HKLM\software\microsoft\windows\currentversion

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\uxtheme.dll

Opens key: HKCU\software\microsoft\windows\currentversion\thememanager

Opens key: HKCU\software\microsoft\ctf\langbaraddin\
Opens key: HKLM\software\microsoft\ctf\langbaraddin\

Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]

Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]

Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\compatibility32[c15f543da83b0ca8766e750f61a8b0f7]

Queries value: HKLM\software\microsoft\windows nt\currentversion\ime

compatibility[c15f543da83b0ca8766e750f61a8b0f7]

Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]

Queries value: HKLM\system\currentcontrolset\control\session

manager[criticalsectiontimeout]

Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]

Queries value: HKCR\interface[interfacehelperdisableal1]
Queries value: HKCR\interface[interfacehelperdisableal1forole32]
Queries value: HKCR\interface[interfacehelperdisabletypelib]

00000000046}[interfacehelperdisableall]

Queries value: HKCR\interface\{00020400-0000-0000-c000-

00000000046}[interfacehelperdisableallforole32]

Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKCU\control panel\desktop[smoothscroll]
Queries value: HKLM\system\setup[systemsetupinprogress]

Queries value:

Queries value:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [enable balloon tips]$

HKCR\interface\{00020400-0000-0000-c000-

Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

Queries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

Queries value: HKLM\software\microsoft\internet explorer[version]

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value:

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000002[packedcatalogitem]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 0000000000008 \ [packed catalog item] \ Queries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]

 $\label{lem:hklm} HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 0000000000011 \ [packed catalog item] \ Queries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
Oueries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[supportednamespace] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ no mespace_catalog \ set alog_entries \ (0000000000001[enabled]) \ details \ de$ Oueries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo] Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace _catalog5 \ catalog_entries \ 000000000002 [library path]$ Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ (catalog_entries \ 0000000000002 \ [displaystring]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily] Oueries value:

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000003 \ [displaystring]$ Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 000000000003 \ [address family]$ Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space _ catalog 5 \ (catalog_entries \ 0000000000003 [supported name space]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000003[version] Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog5 \ catalog_entries \ 10000000000003 \ [storesservice class in fo]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms

shell dlg 2]

HKLM\software\microsoft\ctf\systemshared[cuas] Oueries value: Queries value: HKCU\keyboard layout\toggle[language hotkey] HKCU\keyboard layout\toggle[hotkey] Oueries value: HKCU\keyboard layout\toggle[layout hotkey] Oueries value: Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]

HKLM\software\microsoft\windows nt\currentversion\imm[ime file] Queries value: HKCU\software\microsoft\ctf[disable thread input manager] Oueries value:

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[administrative tools]

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\winlogon[userenvdebuglevel]

HKLM\software\microsoft\windows Queries value:

nt\currentversion\winlogon[chkaccdebuglevel]

Queries value: HKLM\system\currentcontrolset\control\productoptions[producttype] HKCU\software\microsoft\windows\currentversion\explorer\user shell Queries value:

folders[personal]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[local settings]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[rsopdebuglevel]

Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging] Oueries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

HKCU\software\microsoft\windows\currentversion\explorer\user shell

1757981266-507921405-1957994488-1003[profileimagepath]

Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[altstartup]

Queries value: folders[appdata]

Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[cd burning]

Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell

folders[common administrative tools] Oueries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[profilesdirectory]

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\profilelist[allusersprofile]

```
Queries value:
                           HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common altstartup]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common appdata]
                           HKLM\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[common desktop]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common documents]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common favorites]
                           HKLM\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[commonmusic]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[commonpictures]
                           HKLM\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[common programs]
                           HKLM\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[common start menu]
                           HKLM\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[common startup]
                           HKLM\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[common templates]
                           \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} user shell
 Oueries value:
folders[commonvideo]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[cookies]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[desktop]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[favorites]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[fonts]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[history]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[local appdata]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[my music]
 Queries value:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}
folders[my pictures]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[my video]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[nethood]
 Queries value:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}
folders[printhood]
                           HKLM\software\microsoft\windows\currentversion[programfilesdir]
 Oueries value:
 Queries value:
                           HKLM\software\microsoft\windows\currentversion[commonfilesdir]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[programs]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[recent]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[sendto]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[start menul
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[startup]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[templates]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
 Oueries value:
                           HKCU\control panel\desktop[lamebuttontext]
 Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
sans serifl
                           HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\fontsubstitutes[tahoma]
 Queries value:
                           HKCU\software\recovery toolbox for rar[installpath]
                           HKCU\software\recovery toolbox for rar\cbfilename[val0]
 Oueries value:
 Queries value:
                           HKCU\software\recovery toolbox for rar\cbunzipfolder[val0]
 Sets/Creates value:
                           HKCR\.key[]
                           {\tt HKLM \setminus software \setminus microsoft \setminus cryptography \setminus rng[seed]}
 Value changes:
 Value changes:
                           HKCR\.key[]
 Value changes:
                           \label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+explorer\+shell
folders[administrative tools]
 Value changes:
                           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
 Value changes:
                           HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cd
burning]
 Value changes:
                           \label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ windows\+ current version\+ explorer\+ shell
folders[common administrative tools]
 Value changes:
                           \label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ windows\+ current version\+ explorer\+ shell
```

<pre>folders[common appdata]</pre>	
Value changes:	HKLM\software\microsoft\windows\currentversion\explorer\shell
<pre>folders[common desktop]</pre>	
Value changes:	HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common documents	
Value changes:	HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common favorites	
Value changes:	HKLM\software\microsoft\windows\currentversion\explorer\shell
<pre>folders[commonmusic] Value changes:</pre>	HVI M) coftware/microcoft/windows/currentyorsian/evalorer/shall
folders[commonpictures]	HKLM\software\microsoft\windows\currentversion\explorer\shell
Value changes:	HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common programs]	·
Value changes:	HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common start men	'
Value changes:	HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common startup]	·
Value changes:	<pre>HKLM\software\microsoft\windows\currentversion\explorer\shell</pre>
folders[common templates	:1
Value changes:	HKLM\software\microsoft\windows\currentversion\explorer\shell
<pre>folders[commonvideo]</pre>	
Value changes:	HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cookies]	
Value changes:	HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[desktop]	WCD of two and air and of the individual arrangement and air and air and air air
<pre>Value changes: folders[favorites]</pre>	HKCU\software\microsoft\windows\currentversion\explorer\shell
Value changes:	HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[fonts]	Timeo (30) Cwar e (inite) 030) C (withdows (current ver 310) (explorer \shell)
Value changes:	HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[history]	
Value changes:	<pre>HKCU\software\microsoft\windows\currentversion\explorer\shell</pre>
folders[cache]	·
Value changes:	HKCU\software\microsoft\windows\currentversion\explorer\shell
<pre>folders[local appdata]</pre>	
Value changes:	HKCU\software\microsoft\windows\currentversion\explorer\shell folders[my
music]	
Value changes:	HKCU\software\microsoft\windows\currentversion\explorer\shell folders[my
pictures]	II/CII) coftware\microsoft\windows\currentycreion\cyrloren\chall folders[my
Value changes: video]	HKCU\software\microsoft\windows\currentversion\explorer\shell folders[my
Value changes:	HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[nethood]	Theo (30) that the first osof the fi
Value changes:	HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[personal]	
Value changes:	HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[printhood]	
Value changes:	HKCU\software\microsoft\windows\currentversion\explorer\shell
<pre>folders[programs]</pre>	
Value changes:	HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[recent]	
Value changes:	HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[sendto]	III/CII\ coftwara\microcoft\windows\currentyorsi\\\\\\\
Value changes:	HKCU\software\microsoft\windows\currentversion\explorer\shell
<pre>folders[start menu] Value changes:</pre>	HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[startup]	LINCO (201 CHALL CHILTCH 0201 CAMTHAOM2 (CALL LEHEAC) 2TOH (EXPLOYED LI /2HETT
Value changes:	HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[templates]	
• -	