Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 60, Task ID: 239

Task ID: 239 Risk Level:

Date Processed: 2016-04-28 12:53:54 (UTC)

Processing Time: 61.11 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\3967487e5d2dae5d459d7d491277238c.exe"

Sample ID: Type: basic admin Owner:

3967487e5d2dae5d459d7d491277238c Label:

Date Added: 2016-04-28 12:44:55 (UTC) PE32:win32:gui File Type:

File Size: 368304 bytes

3967487e5d2dae5d459d7d491277238c MD5:

f91da84d3f4708c5323fa0ed783ecb6f2e66993db47dadff993c637f5c2a5cd7 SHA256:

Description: None

Pattern Matching Results

2 PE: Nonstandard section

5 Packer: UPX

5 PE: Contains compressed section

Static Events

Anomaly: PE: Contains a virtual section

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

Packer:

Process/Thread Events

Creates process: C:\WINDOWS\Temp\3967487e5d2dae5d459d7d491277238c.exe

["c:\windows\temp\3967487e5d2dae5d459d7d491277238c.exe"]

Named Object Events

Creates mutex: \BaseNamedObjects\3967487e5d2dae5d459d7d491277238c.exeesoc19uK

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

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

1957994488-1003

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

1957994488-1003

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

507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003 \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} Creates semaphore:

Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D} Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57} \BaseNamedObjects\INI-3967487e5d2dae5d459d7d491277238c.data Creates semaphore:

Creates semaphore: \BaseNamedObjects\GR_FileChecker

Creates semaphore: \BaseNamedObjects\GR0

\BaseNamedObjects\GR_FlushingList Creates semaphore: Creates semaphore: \BaseNamedObjects\GR_Write

Creates semaphore: \BaseNamedObjects\GR_GErrMsg \BaseNamedObjects\GR1 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR2 Creates semaphore: \BaseNamedObjects\GR3

\BaseNamedObjects\GR4 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR5 Creates semaphore: \BaseNamedObjects\GR6 Creates semaphore: \BaseNamedObjects\GR7 Creates semaphore: \BaseNamedObjects\GR8 \BaseNamedObjects\GR9 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR10

\BaseNamedObjects\GR11 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR12 Creates semaphore: \BaseNamedObjects\GR13 Creates semaphore: \BaseNamedObjects\GR14

Creates semaphore: \BaseNamedObjects\GR15 Creates semaphore: \BaseNamedObjects\GR16 \BaseNamedObjects\GR17 Creates semaphore: \BaseNamedObjects\GR18 Creates semaphore:

Creates semaphore: \BaseNamedObjects\GR19 Creates semaphore: \BaseNamedObjects\GR20

\BaseNamedObjects\GR21 Creates semaphore: \BaseNamedObjects\GR22 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR23 \BaseNamedObjects\GR24 Creates semaphore: \BaseNamedObjects\GR25 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR26 \BaseNamedObjects\GR27 Creates semaphore: \BaseNamedObjects\GR28 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR29 Creates semaphore: \BaseNamedObjects\GR30 \BaseNamedObjects\GR31 Creates semaphore: Creates semaphore: $\BaseNamedObjects\GR32$ Creates semaphore: \BaseNamedObjects\GR33 Creates semaphore: \BaseNamedObjects\GR34 Creates semaphore: \BaseNamedObjects\GR35 Creates semaphore: \BaseNamedObjects\GR36 Creates semaphore: \BaseNamedObjects\GR37 Creates semaphore: \BaseNamedObjects\GR38 Creates semaphore: \BaseNamedObjects\GR39 Creates semaphore: \BaseNamedObjects\GR40 Creates semaphore: \BaseNamedObjects\GR41 Creates semaphore: \BaseNamedObjects\GR42 Creates semaphore: \BaseNamedObjects\GR43 Creates semaphore: \BaseNamedObjects\GR44 Creates semaphore: \BaseNamedObjects\GR45 \BaseNamedObjects\GR46 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR47 Creates semaphore: \BaseNamedObjects\GR48 \BaseNamedObjects\GR49 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR50 \BaseNamedObjects\GR51 Creates semaphore: \BaseNamedObjects\GR52 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR53 Creates semaphore: \BaseNamedObjects\GR54 **\BaseNamedObjects\GR55** Creates semaphore: Creates semaphore: \BaseNamedObjects\GR56 \BaseNamedObjects\GR57 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR58 Creates semaphore: \BaseNamedObjects\GR59 \BaseNamedObjects\GR60 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR61 Creates semaphore: \BaseNamedObjects\GR62 \BaseNamedObjects\GR63 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR64 \BaseNamedObjects\GR65 Creates semaphore: \BaseNamedObjects\GR66 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR67 Creates semaphore: \BaseNamedObjects\GR68 \BaseNamedObjects\GR69 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR70 \BaseNamedObjects\GR71 Creates semaphore: \BaseNamedObjects\GR72 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR73 \BaseNamedObjects\GR74 Creates semaphore: \BaseNamedObjects\GR75 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR76 \BaseNamedObjects\GR77 Creates semaphore: \BaseNamedObjects\GR78 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR79 Creates semaphore: \BaseNamedObjects\GR80 Creates semaphore: \BaseNamedObjects\GR81 Creates semaphore: \BaseNamedObjects\GR82 Creates semaphore: \BaseNamedObjects\GR83 \BaseNamedObjects\GR84 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR85 Creates semaphore: \BaseNamedObjects\GR86 Creates semaphore: \BaseNamedObjects\GR87 Creates semaphore: \BaseNamedObjects\GR88 Creates semaphore: \BaseNamedObjects\GR89 \BaseNamedObjects\GR90 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR91 \BaseNamedObjects\GR92 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR93 Creates semaphore: \BaseNamedObjects\GR94 Creates semaphore: \BaseNamedObjects\GR95 \BaseNamedObjects\GR96 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR97 \BaseNamedObjects\GR98 Creates semaphore: \BaseNamedObjects\GR99 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR100 Creates semaphore: \BaseNamedObjects\INI-3967487e5d2dae5d459d7d491277238c.data0

```
Creates:
                                     C:\Documents and Settings
  Creates:
                                     C:\Documents and Settings\Admin
                                     C:\Documents and Settings\Admin\Application Data
  Creates:
  Creates:
                                     C:\Documents and Settings\Admin\Application Data\GetRightToGo
  Creates:
                                     C:\Documents and Settings\Admin\Application Data\GetRightToGo\
  Creates:
                                     C:\Documents and Settings\Admin\Application
Data\GetRightToGo\3967487e5d2dae5d459d7d491277238c.data
                                     C:\Documents and Settings\Admin\Application
Data\GetRightToGo\3967487e5d2dae5d459d7d491277238c.data0
                                     C:\WINDOWS\Prefetch\3967487E5D2DAE5D459D7D4912772-2A8E1203.pf
  Opens:
  Opens:
                                     C:\Documents and Settings\Admin
  Opens:
                                     C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
  Opens:
                                     C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
                                     C:\WINDOWS\system32\oledlg.dll
  Opens:
  Opens:
                                     C:\WINDOWS\system32\winspool.drv
  Opens:
                                     C:\WINDOWS\system32\ws2_32.dll
  Opens:
                                     C:\WINDOWS\system32\ws2help.dll
  Opens:
                                     C:\WINDOWS\system32\imm32.dll
  Opens:
                                     C:\WINDOWS\WindowsShell.Manifest
                                     C:\WINDOWS\WindowsShell.Config
  Opens:
  Opens:
                                     C:\WINDOWS\system32\shell32.dll
  Opens:
                                     C:\WINDOWS\system32\SHELL32.dll.124.Manifest
  Opens:
                                     C:\WINDOWS\system32\SHELL32.dll.124.Config
  Opens:
                                     C:\windows\temp\3967487e5d2dae5d459d7d491277238c.exe.2.Manifest
  Opens:
                                     C:\windows\temp\3967487e5d2dae5d459d7d491277238c.exe.3.Manifest
  Opens:
                                     C:\windows\temp\3967487e5d2dae5d459d7d491277238c.exe.Manifest
  Opens:
                                     C:\windows\temp\3967487e5d2dae5d459d7d491277238c.exe.Config
  Opens:
                                     C:\windows\temp\3967487e5d2dae5d459d7d491277238c.exe.1000.Manifest
  Opens:
                                     C:\
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings
                                     C:\WINDOWS\system32\MSCTF.dll
  Opens:
  Opens:
                                     C:\WINDOWS\system32\MSCTFIME.IME
  Opens:
                                     C:\WINDOWS\system32\uxtheme.dll
  Opens:
                                     C:\WINDOWS\system32\MSIMTF.dll
  Opens:
                                     C:\WINDOWS\system32\rpcss.dll
                                     C:\WINDOWS\system32\setupapi.dll
  Opens:
                                     C:\Documents and Settings
  Opens:
  Opens:
                                     C:\Documents and Settings\All Users
                                     C:\Documents and Settings\Admin\Application Data\desktop.ini
  Opens:
                                     C:\Documents and Settings\Admin\Application Data\GetRightToGo
  Opens:
  Opens:
                                     C:\Documents and Settings\Admin\Application
Data\GetRightToGo\3967487e5d2dae5d459d7d491277238c.data
                                     C:\WINDOWS\Temp
  Opens:
  Opens:
                                     C:\WINDOWS\Temp\3967487e5d2dae5d459d7d491277238c.exe
                                     C:\WINDOWS\Temp\163df993-80c0-448a-9917-78c69a8e6968
  Opens:
                                     C:\Documents and Settings\Admin\Application
  Opens:
Data\GetRightToGo\3967487e5d2dae5d459d7d491277238c.data0
  Opens:
                                     C:\Documents and Settings\All Users\Desktop
                                     C:\Documents and Settings\Admin\Desktop\Downloads\
  Opens:
  Opens:
                                     C:\WINDOWS\Fonts\sserife.fon
  Writes to:
                                     C:\Documents and Settings\Admin\Application
Data\GetRightToGo\3967487e5d2dae5d459d7d491277238c.data
  Writes to:
                                     C:\Documents and Settings\Admin\Application
Data\GetRightToGo\3967487e5d2dae5d459d7d491277238c.data0
                                     C:\Documents and Settings\Admin\Application Data\desktop.ini
  Reads from:
  Reads from:
                                     C:\WINDOWS\Temp\3967487e5d2dae5d459d7d491277238c.exe
  Reads from:
                                     C:\Documents and Settings\Admin\Application
Data\GetRightToGo\3967487e5d2dae5d459d7d491277238c.data
  Reads from:
                                     C:\Documents and Settings\Admin\Application
Data\GetRightToGo\3967487e5d2dae5d459d7d491277238c.data0
Windows Registry Events
  Creates key:
                                     HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders
  Creates key:
                                     \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} software \end{tabular} is a simple constant of the constant version \end{tabular} and the constant version \end{tabular} explorer \end{tabular} software \end{tabular} with tabular \end{tabular} and the constant version \end{tabular} explorer \end{tabular} with tabular \end{tabular} and tabular \end{tabular} with tabular \end{tabular} with tabular \end{tabular} explorer \end{tabular} and tabular \end{tabular} and tabular \end{tabular} with tabular \end{tabular} explorer \end{tabular} with tabular \end
806d6172696f}\
                                     HKCU\software\headlight
  Creates kev:
  Creates key:
                                     HKCU\software\headlight\getrighttogo
  Creates key:
                                     HKCU\software\headlight\getrighttogo\sharedconfig
  Creates key:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Creates key:
                                     HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Creates kev:
                                     HKCU\software\headlight\getrighttogo\customizedapps
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens kev:
options\3967487e5d2dae5d459d7d491277238c.exe
  Opens key:
                                     HKLM\system\currentcontrolset\control\terminal server
  Opens key:
```

 $HKLM \ software \ microsoft \ windows \ current version \ side by side \ as sembly storage roots$

HKLM\system\currentcontrolset\control\safeboot\option Opens key: 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 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: 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\msvcrt.dll 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 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: 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 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\shlwapi.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\comctl32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\comdlg32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\oleaut32.dll $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key: options\oledlg.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\winspool.drv 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\system\currentcontrolset\control\error message instrument\ Opens key: $\label{lem:hklm} \verb+Kklm \+ system \+ control \+ error message instrument$ Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ gre_initialize$ Opens kev: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility Opens key: HKLM\software\microsoft\windows nt\currentversion\windows HKLM\software\microsoft\windows\currentversion\explorer\performance Opens key: Opens key: HKCU\ Opens key: HKCU\software\policies\microsoft\control panel\desktop Opens key: HKCU\control panel\desktop Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\advanced}} \\$ Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack HKLM\system\setup Opens key: HKLM\software\microsoft\ole Opens key: Opens key: HKCR\interface Opens key: HKCR\interface\{00020400-0000-0000-c000-00000000046} Opens key: HKLM\software\microsoft\oleaut Opens key: HKLM\software\microsoft\oleaut\userera Opens key: HKCU\software\classes\ HKCU\software\classes\clsid Opens key: Opens key: HKCR\clsid Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer Opens key: $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \policies \network$ Opens key: HKCU\software\microsoft\windows\currentversion\policies\comdlg32 Opens kev: HKLM\svstem\currentcontrolset\control\computername Opens key: $HKLM \verb|\system| current controlset| \verb|\computername| active computername|$ Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctf.dll Opens key: HKLM\software\microsoft\ctf\compatibility\3967487e5d2dae5d459d7d491277238c.exe HKLM\software\microsoft\ctf\systemshared\ Opens key: Opens key: HKCU\keyboard layout\toggle Opens key: HKLM\software\microsoft\ctf\ Opens key: HKLM\software\microsoft\windows nt\currentversion\imm Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\version.dll
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msctfime.ime

HKCU\software\microsoft\ctf Opens key:

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

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

options\uxtheme.dll

Opens key: HKCU\software\microsoft\windows\currentversion\thememanager Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters

Opens key:

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

Opens key:

Opens key:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001 Opens key:

Opens key:

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

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

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens key:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 000000000010$ Opens key:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens key:

Opens key:

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

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ 3967487e5d2 dae 5d459d7d491277238c. exemple \ applications \ applications$ Opens key:

a2d8-08002b30309d}

Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\inprocserver32

Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\setupapi.dll

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

Opens key: HKLM\system\wpa\pnp

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

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

HKLM\system\currentcontrolset\services\tcpip\parameters Opens kev: Opens key: HKLM\software\policies\microsoft\system\dnsclient

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

Opens key: HKLM\software\microsoft\rpc

Opens key: $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabul$

options\3967487e5d2dae5d459d7d491277238c.exe\rpcthreadpoolthrottle Opens kev: HKLM\software\policies\microsoft\windows nt\rpc

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints 2 \ cpc \ volume$

Opens key:

11e3-9fc7-806d6172696f}\

HKCU\software\classes\directory Opens kev:

HKCR\directory Opens key:

Opens key: HKCU\software\classes\directory\curver

Opens key: HKCR\directory\curver Opens key: HKCR\directory\

Opens key: $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ explorer and the software \verb+ windows \verb+ current version \verb+ explorer and the software \verb+ windows \verb+ current version \verb+ explorer and the software \verb+ windows \verb+ current version \verb+ explorer and the software \verb+ windows \verb+ current version \verb+ explorer and the software \verb+ windows \verb+ current version \verb+ explorer and the software \verb+ windows \verb+ current version \verb+ explorer and the software \verb+ windows \verb+ explorer and the software explorer and t$ Opens key: HKCU\software\microsoft\windows\currentversion\explorer\ Opens key: HKCU\software\microsoft\windows\currentversion\policies\system

```
HKCU\software\classes\directory\shellex\iconhandler
   Opens key:
   Opens key:
                                                  HKCR\directorv\shellex\iconhandler
   Opens key:
                                                  HKCU\software\classes\directory\clsid
   Opens key:
                                                  HKCR\directory\clsid
   Opens key:
                                                  HKCU\software\classes\folder
   Opens key:
                                                  HKCR\folder
   Opens key:
                                                  HKCU\software\classes\folder\clsid
                                                  HKCR\folder\clsid
   Opens key:
   Opens key:
                                                  HKCU\software
   Opens key:
                                                  HKCU\software\classes\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder
   Opens key:
                                                  HKCR\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder
   Opens key:
HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ objects \ \{450d8fba-ad25-11d0-d148fba-d25-11d0-d148fba-d25-11d0-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148fba-d25-d148
98a8-0800361b1103}
   Opens key:
                                                  HKCU\software\microsoft\windows\currentversion\policies\nonenum
   Opens kev:
                                                  HKI M\software\microsoft\windows\currentversion\policies\nonenum
   Opens key:
                                                  HKCU\software\microsoft\windows\currentversion\explorer\clsid\{450d8fba-
ad25-11d0-98a8-0800361b1103}\shellfolder
                                                  HKLM \ software \ microsoft \ windows \ current version \ explorer \ clsid \ \{450d8fba-microsoft \ windows \ explorer \
   Opens key:
ad25-11d0-98a8-0800361b1103}\shellfolder
   Queries value:
                                                  HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
   Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [transparentenabled]
                                                  HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
   Queries value:
   Queries value:
                                                  HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
   Queries value:
                                                  HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
                                                  HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\compatibility32[3967487e5d2dae5d459d7d491277238c]
                                                 HKLM\software\microsoft\windows nt\currentversion\ime
   Queries value:
compatibility[3967487e5d2dae5d459d7d491277238c]
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
                                                  HKCU\control panel\desktop[multiuilanguageid]
   Oueries value:
   Queries value:
                                                  HKCU\control panel\desktop[smoothscroll]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
                                                  HKLM\system\setup[systemsetupinprogress]
                                                  HKLM\system\currentcontrolset\control\session
   Queries value:
manager[criticalsectiontimeout]
                                                  HKLM\software\microsoft\ole[rwlockresourcetimeout]
   Queries value:
                                                  HKCR\interface[interfacehelperdisableall]
   Oueries value:
                                                  HKCR\interface[interfacehelperdisableallforole32]
   Queries value:
                                                  HKCR\interface[interfacehelperdisabletypelib]
   Oueries value:
                                                  HKCR\interface\{00020400-0000-0000-c000-
   Queries value:
00000000046}[interfacehelperdisableall]
   Queries value:
                                                  HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableallforole32]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\policies\explorer[norun]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nodrives]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetconnectdisconnect]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[norecentdocshistory]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noclose]
   Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                                                  HKLM\software\microsoft\ctf\systemshared[cuas]
   Queries value:
                                                  HKCU\keyboard layout\toggle[language hotkey]
   Oueries value:
                                                  HKCU\keyboard layout\toggle[hotkey]
   Oueries value:
                                                  HKCU\keyboard layout\toggle[layout hotkey]
   Oueries value:
   Queries value:
                                                  HKLM\software\microsoft\ctf[enableanchorcontext]
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
   Queries value:
                                                  HKCU\software\microsoft\ctf[disable thread input manager]
   Oueries value:
                                                  HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
   Queries value:
                                                  HKCU\control panel\desktop[lamebuttontext]
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
   Oueries value:
```

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

Oueries value:

Oueries value:

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]
 Oueries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Queries value:
- Oueries value:

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Queries 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\000000000001[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
 Oueries 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\0000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Oueries 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] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring] Queries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000003 \ [providerid] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 0000000000003 \ [enabled] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
 Oueries value:
- HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood]
 Oueries value:
- HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
 Queries value:
- HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] Oueries value:
- $\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \policies \explorer \cite{thm:linear} no common groups \cite{thm:linear} and \cite{$
 - Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell

folders[common desktop]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]

Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]

HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[] Queries value:

Oueries value: HKLM\system\wpa\pnp[seed] Oueries value: HKLM\system\setup[osloaderpath] Queries value: HKLM\system\setup[systempartition]

Oueries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]

Oueries value:

HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]

Oueries value:

HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]

HKLM\software\microsoft\windows\currentversion\setup[drivercachepath] Queries value:

Queries value: HKLM\software\microsoft\windows\currentversion[devicepath] HKLM\software\microsoft\windows\currentversion\setup[loglevel] Oueries value: Queries value: HKLM\software\microsoft\windows\currentversion\setup[logpath] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [domain]$

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

Queries value:

11e3-9fc7-806d6172696f}[data]

Queries value:

11e3-9fc7-806d6172696f}[generation]

Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]

HKCU\software\microsoft\windows\currentversion\explorer[shellstate]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon]

HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]

HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]

Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip] Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]

Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]

HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]

Queries value:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [show superhidden]$

HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]

Oueries value:

 $\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} nonetcrawling \cite{tabular} and \cit$

HKCR\directory[docobject] Queries value: Oueries value: HKCR\directory[browseinplace] Queries value: HKCR\directory[isshortcut] HKCR\directory[alwaysshowext] Oueries value: Queries value: HKCR\directory[nevershowext]

HKCU\software\headlight\getrighttogo\sharedconfig[useloadimage] Oueries value: HKCU\software\headlight\getrighttogo\sharedconfig[doxpthemes] Oueries value: Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[appdata]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache] Oueries value: HKCU\software\headlight\getrighttogo\sharedconfig[debug]

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

folders[desktop]

Queries value: HKCU\software\headlight\getrighttogo\sharedconfig[screenreader]

HKCR\clsid\{450d8fba-ad25-11d0-98a8-Oueries value:

0800361b1103}\shellfolder[wantsforparsing]

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

folders[personal]

Queries value: HKCR\clsid\{450d8fba-ad25-11d0-98a8-

0800361b1103}\shellfolder[attributes]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{450d8fba-ad25-11d0-98a8-0800361b1103\}]$

Sets/Creates value:

HKCU\software\headlight\getrighttogo\customizedapps[3967487e5d2dae5d459d7d491277238c]

Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[busypause]

Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[filecache]

Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[filecachekb]

Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[rollback]

Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[dotgetright]

Value changes: HKLM\software\microsoft\cryptography\rng[seed]

Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell

folders[common desktop]

Value changes:

806d6172696f}[baseclass]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[appdata]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[desktop]