Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 6, Task ID: 22

Task ID: 22 Risk Level: 5

Date Processed: 2016-04-28 12:46:41 (UTC)

Processing Time: 61.07 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe"

Sample ID: 6
Type: basic
Owner: admin

Label: 70c87e532c1ff4ae687b26c4224aa435

Date Added: 2016-04-28 12:44:50 (UTC)
File Type: PE32:win32:gui

File Type: PE32:win32:gui File Size: 368256 bytes

MD5: 70c87e532c1ff4ae687b26c4224aa435

SHA256: 28b52897659cf99851f39f4f2c0c423f55a328ba2de1f3da894a85ba624b6e9b

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: UPX

Process/Thread Events

Creates process: C:\WINDOWS\Temp\70c87e532c1ff4ae687b26c4224aa435.exe

["c:\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe"]

Named Object Events

Creates mutex: \BaseNamedObjects\70c87e532c1ff4ae687b26c4224aa435.exeIrjLp11A

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

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

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

Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.EOG

Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} \Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D} \Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57} \BaseNamedObjects\INI-70c87e532c1ff4ae687b26c4224aa435.data

Creates semaphore: \BaseNamedObjects\GR_FileChecker

Creates semaphore: \BaseNamedObjects\GRO

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

Creates semaphore: \BaseNamedObjects\GR1 Creates semaphore: \BaseNamedObjects\GR2 \BaseNamedObjects\GR3 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR4 Creates semaphore: \BaseNamedObjects\GR5 Creates semaphore: \BaseNamedObjects\GR6 Creates semaphore: \BaseNamedObjects\GR7 \BaseNamedObjects\GR8 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR9 \BaseNamedObjects\GR10 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR11 Creates semaphore: \BaseNamedObjects\GR12 Creates semaphore: \BaseNamedObjects\GR13 Creates semaphore: \BaseNamedObjects\GR14 Creates semaphore: \BaseNamedObjects\GR15 \BaseNamedObjects\GR16 Creates semaphore: \BaseNamedObjects\GR17 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR18 Creates semaphore: \BaseNamedObjects\GR19

\BaseNamedObjects\GR20 Creates semaphore: \BaseNamedObjects\GR21 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR22 \BaseNamedObjects\GR23 Creates semaphore: \BaseNamedObjects\GR24 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR25 \BaseNamedObjects\GR26 Creates semaphore: \BaseNamedObjects\GR27 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR28 \BaseNamedObjects\GR29 Creates semaphore: \BaseNamedObjects\GR30 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR31 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 \BaseNamedObjects\GR39 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR40 Creates semaphore: \BaseNamedObjects\GR41 Creates semaphore: \BaseNamedObjects\GR42 Creates semaphore: \BaseNamedObjects\GR43 \BaseNamedObjects\GR44 Creates semaphore: **\BaseNamedObjects\GR45** Creates semaphore: Creates semaphore: \BaseNamedObjects\GR46 Creates semaphore: \BaseNamedObjects\GR47 \BaseNamedObjects\GR48 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR49 \BaseNamedObjects\GR50 Creates semaphore: \BaseNamedObjects\GR51 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR52 Creates semaphore: \BaseNamedObjects\GR53 \BaseNamedObjects\GR54 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR55 \BaseNamedObjects\GR56 Creates semaphore: \BaseNamedObjects\GR57 Creates semaphore: \BaseNamedObjects\GR58 Creates semaphore: \BaseNamedObjects\GR59 Creates semaphore: Creates semaphore: **\BaseNamedObjects\GR60** \BaseNamedObjects\GR61 Creates semaphore: \BaseNamedObjects\GR62 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR63 \BaseNamedObjects\GR64 Creates semaphore: \BaseNamedObjects\GR65 Creates semaphore: Creates semaphore: **\BaseNamedObjects\GR66** Creates semaphore: \BaseNamedObjects\GR67 \BaseNamedObjects\GR68 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR69 \BaseNamedObjects\GR70 Creates semaphore: \BaseNamedObjects\GR71 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR72 \BaseNamedObjects\GR73 Creates semaphore: \BaseNamedObjects\GR74 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR75 \BaseNamedObjects\GR76 Creates semaphore: \BaseNamedObjects\GR77 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR78 Creates semaphore: \BaseNamedObjects\GR79 Creates semaphore: \BaseNamedObjects\GR80 Creates semaphore: \BaseNamedObjects\GR81 \BaseNamedObjects\GR82 Creates semaphore: \BaseNamedObjects\GR83 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR84 \BaseNamedObjects\GR85 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR86 Creates semaphore: \BaseNamedObjects\GR87 Creates semaphore: \BaseNamedObjects\GR88 \BaseNamedObjects\GR89 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR90 \BaseNamedObjects\GR91 Creates semaphore: \BaseNamedObjects\GR92 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR93 Creates semaphore: \BaseNamedObjects\GR94 \BaseNamedObjects\GR95 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR96 \BaseNamedObjects\GR97 Creates semaphore: \BaseNamedObjects\GR98 Creates semaphore: Creates semaphore: \BaseNamedObjects\GR99 Creates semaphore: \BaseNamedObjects\GR100

Creates semaphore: \BaseNamedObjects\INI-70c87e532c1ff4ae687b26c4224aa435.data0

File System Events

C:\Documents and Settings Creates: C:\Documents and Settings\Admin C:\Documents and Settings\Admin\Application Data Creates: C:\Documents and Settings\Admin\Application Data\GetRightToGo Creates: C:\Documents and Settings\Admin\Application Data\GetRightToGo\ Creates: Creates: C:\Documents and Settings\Admin\Application Data\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data C:\Documents and Settings\Admin\Application Data\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data0 C:\WINDOWS\Prefetch\70C87E532C1FF4AE687B26C4224AA-32123872.pf Opens: C:\Documents and Settings\Admin Opens: Opens: 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\system32\oledlg.dll Opens: C:\WINDOWS\system32\winspool.drv Opens: Opens: C:\WINDOWS\system32\ws2_32.dll Opens: C:\WINDOWS\system32\ws2help.dll Opens: C:\WINDOWS\system32\imm32.dll Opens: C:\WINDOWS\WindowsShell.Manifest Opens: C:\WINDOWS\WindowsShell.Config Opens: C:\WINDOWS\system32\shell32.dll Opens: C:\WINDOWS\system32\SHELL32.dll.124.Manifest Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config $C: \verb|\windows| temp| 70c87e532c1ff4ae687b26c4224aa435.exe.2. Manifest| \\$ Opens: Opens: C:\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe.3.Manifest Opens: C:\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe.Manifest Opens: C:\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe.Config Opens: C:\windows\temp\70c87e532c1ff4ae687b26c4224aa435.exe.1000.Manifest Opens: Opens: C:\Documents and Settings\Admin\Local Settings Opens: C:\WINDOWS\system32\MSCTF.dll Opens: C:\WINDOWS\system32\MSCTFIME.IME C:\WINDOWS\system32\uxtheme.dll Opens: Opens: C:\WINDOWS\system32\MSIMTF.dll Opens: C:\WINDOWS\system32\rpcss.dll Opens: C:\WINDOWS\system32\setupapi.dll Opens: C:\Documents and Settings Opens: C:\Documents and Settings\All Users C:\Documents and Settings\Admin\Application Data\desktop.ini Opens: Opens: C:\Documents and Settings\Admin\Application Data\GetRightToGo C:\Documents and Settings\Admin\Application Opens: Data\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data C:\WINDOWS\Temp Opens: Opens: C:\WINDOWS\Temp\70c87e532c1ff4ae687b26c4224aa435.exe Opens: C:\WINDOWS\Temp\636ef357-6371-4294-8daf-897cb5ad0051 C:\Documents and Settings\Admin\Application Data\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data0 Opens: C:\Documents and Settings\All Users\Desktop C:\Documents and Settings\Admin\Desktop\Downloads\ Opens: C:\WINDOWS\Fonts\sserife.fon Opens: Writes to: C:\Documents and Settings\Admin\Application Data\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data C:\Documents and Settings\Admin\Application Writes to: Data\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data0 C:\Documents and Settings\Admin\Application Data\desktop.ini Reads from: C:\WINDOWS\Temp\70c87e532c1ff4ae687b26c4224aa435.exe Reads from: Reads from: C:\Documents and Settings\Admin\Application Data\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data C:\Documents and Settings\Admin\Application Reads from: Data\GetRightToGo\70c87e532c1ff4ae687b26c4224aa435.data0

Windows Registry Events

Creates key:	<pre>HKLM\software\microsoft\windows\currentversion\explorer\user shell</pre>
folders	
Creates key:	<pre>HKLM\software\microsoft\windows\currentversion\explorer\shell folders</pre>
Creates key:	
HKCU\software\micro	soft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-
806d6172696f}\	
Creates key:	HKCU\software\headlight
Creates key:	<pre>HKCU\software\headlight\getrighttogo</pre>
Creates key:	<pre>HKCU\software\headlight\getrighttogo\sharedconfig</pre>
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\explorer\user shell</pre>
folders	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\explorer\shell folders</pre>
Creates key:	<pre>HKCU\software\headlight\getrighttogo\customizedapps</pre>
Opens key:	<pre>HKLM\software\microsoft\windows nt\currentversion\image file execution</pre>

options\70c87e532c1ff4ae687b26c4224aa435.exe Opens key: HKLM\system\currentcontrolset\control\terminal server

Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots Opens kev: HKLM\system\currentcontrolset\control\safeboot\option HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: 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 Opens key: HKLM\ HKLM\software\microsoft\windows nt\currentversion\diagnostics Opens key: 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 key: HKLM\system\currentcontrolset\control\session manager $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key: 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 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\gdi32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\shell32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comdlg32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key: options\oleaut32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\oledlg.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\winspool.drv $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ 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: HKLM\svstem\currentcontrolset\control\error message instrument Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 HKLM\software\microsoft\windows nt\currentversion\ime compatibility Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\windows Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ performance$ Opens key: HKCU\ Opens key: HKCU\software\policies\microsoft\control panel\desktop Opens key: HKCU\control panel\desktop Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack Opens key: HKLM\system\setup Opens key: HKLM\software\microsoft\ole Opens key: HKCR\interface Opens key: HKCR\interface\{00020400-0000-0000-c000-00000000046} Opens key: HKLM\software\microsoft\oleaut HKLM\software\microsoft\oleaut\userera Opens key: Opens key: HKCU\software\classes\ Opens key: HKCU\software\classes\clsid

Opens key: HKCR\clsid

Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\network
Opens key: HKCU\software\microsoft\windows\currentversion\policies\comdlg32

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

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msctf.dll

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus ctf \setminus compatibility \setminus 70c87e532c1ff4ae687b26c4224aa435.exe$

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

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

Opens key: HKCU\software\microsoft\ctf

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

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

options\uxtheme.dll

 $\label{lem:control} Opens~key: & HKCU\software\microsoft\windows\currentversion\thememanager \\ Opens~key: & HKLM\system\currentcontrolset\services\winsock2\parameters \\ \end{tabular}$

Opens key:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004

Opens key:

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010

 $\label{local-protocol} HKLM \system \current controlset \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \000000000011 \parameters \end{subarray}.$ Opens key:

 $HKL\dot{M} \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace_catalog 5$

Opens key:

 $\label{lem:hklm} \begin{tabular}{ll} HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004\\ \end{tabular}$

Opens key:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003

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

 $HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ 70c87e532c1ff4ae687b26c4224aa435.exe. Opens key:$

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

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

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

Opens key: HKLM\software\microsoft\rpc

 $Opens\ key: \\ HKLM\software\mbox{microsoft\windows}\ nt\current\version\box{\sc file}\ execution$

 $options \verb|\| 70c87e532c1ff4ae687b26c4224aa435.exe \verb|\| rpcthreadpoolthrottle \\ Opens key: HKLM \verb|\| software \verb|\| policies \verb|\| microsoft \verb|\| windows nt \verb|\| rpc \\ HKLM \verb|\| software \verb|\| software \verb|\| software \\ HKLM \verb|\| software \| software \\ HKLM \verb|\| software \| software \\ HKLM \verb|\| software \| software \| software \\ HKLM \verb|\| software \| software \\ HKLM \verb|\| software \| software \| software \| software \| software \\ HKLM \verb|\| software \| software \|$

Opens key:

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

Opens key:

 $\label{thm:constraint} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ff 90255c2-6bc4-1000 \columnwidth \col$

11e3-9fc7-806d6172696f}\

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

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

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

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\ Opens key: HKCU\software\microsoft\windows\currentversion\policies\system

Opens kev: HKCU\software\classes\directory\shellex\iconhandler

Opens key: HKCR\directory\shellex\iconhandler Opens key: HKCU\software\classes\directory\clsid

Opens key: HKCR\directory\clsid Opens key: HKCU\software\classes\folder

HKCR\folder Opens key:

Opens key: HKCU\software\classes\folder\clsid

Opens key: HKCR\folder\clsid HKCU\software Opens key:

Opens key: HKCU\software\classes\clsid\{450d8fba-ad25-11d0-98a8-

0800361b1103}\shellfolder

HKCR\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder Opens key:

Opens key:

HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{450d8fba-ad25-11d0-

98a8-0800361b1103}

Opens key: HKCU\software\microsoft\windows\currentversion\policies\nonenum Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{450d8fba-microsoft \setminus explorer \setminus clsid \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid \setminus explorer \setminus clsid$ Opens key:

ad25-11d0-98a8-0800361b1103}\shellfolder

Opens key:

ad25-11d0-98a8-0800361b1103}\shellfolder

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

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

Queries value:

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

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

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

 $nt \verb|\currentversion| compatibility 32 [70c87e532c1ff4ae687b26c4224aa435]| \\$

 ${\it HKLM \ } software \verb|\microsoft \ | microsoft \ | micr$ Queries value:

compatibility[70c87e532c1ff4ae687b26c4224aa435]

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

HKCU\control panel\desktop[multiuilanguageid] Queries value: HKCU\control panel\desktop[smoothscroll] Queries value:

Oueries value:

Oueries value: HKLM\svstem\setup[svstemsetupinprogress] Oueries value: HKLM\system\currentcontrolset\control\session

manager[criticalsectiontimeout]

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

HKCR\interface[interfacehelperdisableall] Queries value: HKCR\interface[interfacehelperdisableallforole32] Oueries value: HKCR\interface[interfacehelperdisabletypelib]

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

00000000046}[interfacehelperdisableall] HKCR\interface\{00020400-0000-0000-c000-Oueries value:

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:

Queries value:

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

Oueries value:

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

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

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

Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]

Queries value: HKCU\control panel\desktop[lamebuttontext]

Oueries value:

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

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]

Queries value:

Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 [num_catalog_entries]$

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
 Oueries 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]
 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]
 Queries 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]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[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\000000000001[enabled]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- Queries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[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\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
 Oueries value:
- $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2_32 spin count]$

Queries value:

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

Queries value:

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

Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common desktop] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders] HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[] Oueries value: Oueries value: HKLM\system\wpa\pnp[seed] Queries value: HKLM\system\setup[osloaderpath] Oueries 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] Oueries value: HKLM\software\microsoft\windows\currentversion\setup[drivercachepath] Oueries value: HKLM\software\microsoft\windows\currentversion[devicepath] Queries value: HKLM\software\microsoft\windows\currentversion\setup[loglevel] Queries value: HKLM\software\microsoft\windows\currentversion\setup[logpath] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] ${\tt HKLM \backslash system \backslash current control set \backslash services \backslash tcpip \backslash parameters [domain]}$ Queries value: Queries value: HKLM\software\microsoft\rpc[maxrpcsize] Oueries value: $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{f90255c2-6bc4-f9025fc4-f$ 11e3-9fc7-806d6172696f}[data] Oueries value: 11e3-9fc7-806d6172696f}[generation] Queries value: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [dontshow superhidden]$ Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate] Oueries value: Oueries value: $\label{thm:linear} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| policies \verb|\explorer| [noactive desktop] \end{tabular}$ HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess] HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] Oueries value: Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext] HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons] 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] Oueries value: Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]

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

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

folders[appdata]
Queries value:

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

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

folders[desktop]

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

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

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:

 $HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\, \{450d8fba-ad25-11d0-98a8-450d8fba-9840d8fba-9840d8fba-9840d8fba-9840d8fba-9840d8fba-9840d8fba-9840d8fba-9840d8fba-9840d8fba-9840d8fba-9840d8fba-9840d8fba-9840d8fb$

0800361b1103}]
Sets/Creates value:

HKCU\software\headlight\getrighttogo\customizedapps[70c87e532c1ff4ae687b26c4224aa435]

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:

 $HKCU \ software \ microsoft \ windows \ current version \ lex plorer \ mountpoints \ 2 \ \{f90255c2-6bc4-11e3-9fc7-6bc4-11e3-$

806d6172696f}[baseclass]

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

folders[appdata]

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

folders[desktop]