

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3322, Task ID: 796

Task ID:	796
Risk Level:	6
Date Processed:	2016-05-18 10:39:12 (UTC)
Processing Time:	9.44 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\0f31e2adf1807f61e5d6989596ebfb36.exe"
Sample ID:	3322
Type:	basic
Owner:	admin
Label:	0f31e2adf1807f61e5d6989596ebfb36
Date Added:	2016-05-18 10:30:50 (UTC)
File Type:	PE32:win32:gui
File Size:	403680 bytes
MD5:	0f31e2adf1807f61e5d6989596ebfb36
SHA256:	463ad234a346831c72a1e5c1a0ea1d410820651860165d642b04d72a74ba6066
Description:	None

Pattern Matching Results

2	PE: Nonstandard section
6	Creates task in the task scheduler
6	Creates executable in application data folder

Static Events

Anomaly:	PE: No DOS stub
Anomaly:	PE: Contains one or more non-standard sections

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\0f31e2adf1807f61e5d6989596ebfb36.exe
["c:\windows\temp\0f31e2adf1807f61e5d6989596ebfb36.exe"]	
Terminates process:	C:\WINDOWS\Temp\0f31e2adf1807f61e5d6989596ebfb36.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
Creates mutex:	\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates event:	\BaseNamedObjects\userenv: User Profile setup event
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Creates:	C:\Documents and Settings\All Users\Application Data\Mozilla
Creates:	C:\Documents and Settings\All Users\Application Data\Mozilla\rujzyrj.exe
Creates:	C:\WINDOWS\Tasks\rpxkag.job
Opens:	C:\WINDOWS\Prefetch\0F31E2ADF1807F61E5D6989596EBF-29630DBE.pf
Opens:	C:\Documents and Settings\Admin

Opens:	C:\WINDOWS\system32\crypt32.dll
Opens:	C:\WINDOWS\system32\msasn1.dll
Opens:	C:\WINDOWS\system32\ws2_32.dll
Opens:	C:\WINDOWS\system32\ws2help.dll
Opens:	C:\WINDOWS\Temp\0f31e2adf1807f61e5d6989596ebfb36.exe
Opens:	C:\WINDOWS\system32\imm32.dll
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\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
Opens:	C:\WINDOWS\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config
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\MSCTF.dll
Opens:	C:\WINDOWS\system32\MSCTFIME.IME
Opens:	C:\
Opens:	C:\Documents and Settings
Opens:	C:\Documents and Settings\All Users
Opens:	C:\Documents and Settings\All Users\Application Data\Mozilla
Opens:	C:\WINDOWS\system32\rpcss.dll
Opens:	C:\WINDOWS\system32\clbcatq.dll
Opens:	C:\WINDOWS\system32\comres.dll
Opens:	C:\WINDOWS\Registration\R0000000000007.clb
Opens:	C:\WINDOWS\system32\mstask.dll
Opens:	C:\WINDOWS\system32\mstask.dll.2.Manifest
Opens:	C:\WINDOWS\system32\mstask.dll.2.Config
Opens:	C:\WINDOWS\system32\ntdsapi.dll
Opens:	C:\WINDOWS\system32\dnsapi.dll
Opens:	C:\WINDOWS\system32\netapi32.dll
Opens:	C:\WINDOWS\Tasks\rpxkag.job
Opens:	C:\WINDOWS\Tasks
Writes to:	C:\Documents and Settings\All Users\Application Data\Mozilla\rujzyrj.exe
Writes to:	C:\WINDOWS\Tasks\rpxkag.job
Reads from:	C:\WINDOWS\Temp\0f31e2adf1807f61e5d6989596ebfb36.exe
Reads from:	C:\WINDOWS\Registration\R0000000000007.clb

Windows Registry Events

Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\0f31e2adf1807f61e5d6989596ebfb36.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
Opens key:	HKLM\
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\gdi32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution

options\user32.dll	
Opens key:	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\msasn1.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\crypt32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
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\system\currentcontrolset\control\error message instrument
Opens key:	HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key:	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
Opens key:	HKLM\system\currentcontrolset\services\crypt32\performance
Opens key:	HKLM\software\microsoft\windows nt\currentversion\msasn1
Opens key:	HKCU\
Opens key:	HKCU\software\policies\microsoft\control panel\desktop
Opens key:	HKCU\control panel\desktop
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll	
Opens key:	HKLM\software\microsoft\windows\currentversion\explorer\performance
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll	
Opens key:	HKLM\system\setup
Opens key:	
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll	
Opens key:	HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key:	HKLM\software\microsoft\windows nt\currentversion\languagepack
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll	
Opens key:	HKLM\software\microsoft\ole
Opens key:	HKCR\interface
Opens key:	HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll	
Opens key:	HKLM\software\microsoft\oleaut
Opens key:	HKLM\software\microsoft\oleaut\userera
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll	
Opens key:	
HKLM\software\microsoft\ctf\compatibility\0f31e2adf1807f61e5d6989596ebfb36.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\msctftime.ime	
Opens key:	HKCU\software\microsoft\ctf
Opens key:	HKLM\software\microsoft\ctf\systemshared

Opens key:	HKLM\software\microsoft\windows\currentversion\explorer\shell folders
Opens key:	HKLM\software\microsoft\cryptography
Opens key:	HKLM\software\microsoft\com3
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comres.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\clbcatq.dll	
Opens key:	HKLM\software\microsoft\com3\debug
Opens key:	HKCU\software\classes\
Opens key:	HKLM\software\classes
Opens key:	HKU\
Opens key:	HKCR\clsid
Opens key:	HKCU\software\classes\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}
Opens key:	HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}
Opens key:	HKCU\software\classes\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\treatas
Opens key:	HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\treatas
Opens key:	HKCU\software\classes\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprocserver32
Opens key:	HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprocserver32
Opens key:	HKCU\software\classes\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprocserverx86
Opens key:	HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprocserverx86
Opens key:	HKCU\software\classes\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\localserver32
Opens key:	HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\localserver32
Opens key:	HKCU\software\classes\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprochandler32
Opens key:	HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprochandler32
Opens key:	HKCU\software\classes\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprochandlerx86
Opens key:	HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprochandlerx86
Opens key:	HKCU\software\classes\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\localserver
Opens key:	HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\localserver
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\mpr.dll	
Opens key:	HKLM\system\currentcontrolset\control\networkprovider\hworder
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.dll	
Opens key:	HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key:	HKLM\software\policies\microsoft\windows nt\dnsclient
Opens key:	HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netapi32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wldap32.dll	
Opens key:	HKLM\system\currentcontrolset\services\ldap
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdsapi.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll	
Opens key:	HKLM\system\currentcontrolset\control\productoptions
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\image file execution
options\mstask.dll	
Opens key:	HKLM\software\microsoft\schedulingagent
Opens key:	HKLM\system\currentcontrolset\control\nls\locale
Opens key:	HKLM\system\currentcontrolset\control\nls\locale\alternate sorts

Opens key: HKLM\system\currentcontrolset\control\nls\language groups
 Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
 Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-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: HKCU\software\classes\drive\shellex\folderextensions
 Opens key: HKCR\drive\shellex\folderextensions
 Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
 Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
 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\0f31e2adf1807f61e5d6989596ebfb36.exe\pcthreadpoolthrottle
 Opens key: HKLM\software\policies\microsoft\windows nt\rpc
 Opens key: HKLM\system\currentcontrolset\control\computername
 Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
 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[0f31e2adf1807f61e5d6989596ebfb36]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[0f31e2adf1807f61e5d6989596ebfb36]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
 Queries value: HKCU\control panel\desktop[multiuilanguageid]
 Queries value: HKLM\system\setup[systemsetupinprogress]
 Queries value: HKCU\control panel\desktop[smoothscroll]
 Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
 Queries value: HKLM\system\currentcontrolset\control\session manager[criticalsectiontimeout]
 Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]
 Queries value: HKCR\interface[interfacehelperdisableall]
 Queries value: HKCR\interface[interfacehelperdisableallforole32]
 Queries value: HKCR\interface[interfacehelperdisabletypelib]
 Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableall]
 Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableallforole32]
 Queries value: HKLM\software\microsoft\ctf\systemshared[cuas]
 Queries value: HKCU\keyboard layout\toggle[language hotkey]
 Queries value: HKCU\keyboard layout\toggle[hotkey]
 Queries value: HKCU\keyboard layout\toggle[layout hotkey]
 Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
 Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
 Queries value: HKLM\software\microsoft\windows\currentversion\explorer\shell folders[common appdata]
 Queries value: HKLM\software\microsoft\cryptography[machineguid]
 Queries value: HKLM\software\microsoft\com3[com+enabled]
 Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
 Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]

Queries value: HKLM\software\microsoft\com3[regdbversion]
Queries value: HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprocserver32[]
Queries value: HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}[appid]
Queries value: HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprocserver32[threadingmodel]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[prioritizercorddata]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizercorddata]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[appendtomultilabelname]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[screenbadtlds]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[screenunreachableservers]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[filterclusterip]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[waitfornameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[usedns]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[usehostsfile]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablenynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerprimaryname]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerreverselookup]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerwanadapters]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationttl]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]

Queries value:
 HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationmaxaddresscount]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressesstoregister]
 Queries value:
 HKLM\system\currentcontrolset\services\dnsCache\parameters[updatesecuritylevel]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Queries value:
 HKLM\system\currentcontrolset\services\dnsCache\parameters[updatezoneexcludefile]
 Queries value:
 HKLM\system\currentcontrolset\services\dnsCache\parameters[updatetopleveldomainzones]
 Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[dnstest]
 Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachesize]
 Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachettl]
 Queries value:
 HKLM\system\currentcontrolset\services\dnsCache\parameters[maxnegativecachettl]
 Queries value:
 HKLM\system\currentcontrolset\services\dnsCache\parameters[adapertimeoutlimit]
 Queries value:
 HKLM\system\currentcontrolset\services\dnsCache\parameters[serverprioritytimelimit]
 Queries value:
 HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachedsockets]
 Queries value:
 HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastlistenlevel]
 Queries value:
 HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastsendlevel]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
 Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\winlogon[userenvdebuglevel]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\winlogon[chkaccdebuglevel]
 Queries value: HKLM\system\currentcontrolset\control\productoptions[producttype]
 Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
 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]
 Queries value: HKLM\software\microsoft\schedulingagent[tasksfolder]
 Queries value: HKLM\software\microsoft\schedulingagent[notifyontaskmiss]
 Queries value: HKLM\software\microsoft\schedulingagent[viewhiddentasks]
 Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
 Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
 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]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]

Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
Queries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}[drivemask]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]