Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 242, Task ID: 967

Task ID:	967
Risk Level:	5
Date Processed:	2016-04-28 13:14:16 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\d0d59c2e7bbd82b1db28d7f2d0381f4c.exe"
Sample ID:	242
Type:	basic
Owner:	admin
Label:	d0d59c2e7bbd82b1db28d7f2d0381f4c
Date Added:	2016-04-28 12:45:15 (UTC)
File Type:	PE32:win32:gui
File Size:	897024 bytes
MD5:	d0d59c2e7bbd82b1db28d7f2d0381f4c
SHA256:	babc3284e3597c96f318c4471c7cf4995b42280471808111ca6aeb5d9cc53c92
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\d0d59c2e7bbd82b1db28d7f2d0381f4c.exe ["c:\windows\temp\d0d59c2e7bbd82b1db28d7f2d0381f4c.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-1-5-21-1757981266-507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex: \BaseNamedObjects\Window_Washer_Rules
Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Opens: C:\WINDOWS\Prefetch\D0D59C2E7BBD82B1DB28D7F2D0381-2439292C.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\imm32.dll
Opens: C:\WINDOWS\system32\comctl32.dll
Opens: C:\WINDOWS\system32\comctl32.dll.124.Manifest

Opens: C:\WINDOWS\system32\comctl32.dll.124.Config
Opens: C:\WINDOWS\system32\shell32.dll
Opens: C:\WINDOWS\system32\Shell32.dll.124.Manifest
Opens: C:\WINDOWS\system32\Shell32.dll.124.Config
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\URLMON.DLL.123.Manifest
Opens: C:\WINDOWS\system32\URLMON.DLL.123.Config
Opens: C:\WINDOWS\system32\wininet.dll.123.Manifest
Opens: C:\WINDOWS\system32\wininet.dll.123.Config
Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\WINDOWS\system32\MSCTFIME.IME
Opens: C:\Languages\
Opens: C:\WINDOWS\system32\kbdus.dll
Opens: C:\
Opens: C:\WINDOWS\system32\rpcss.dll
Opens: C:\WINDOWS\system32\winlogon.exe
Opens: C:\WINDOWS\system32\xpsp2res.dll
Opens: C:\recycled\
Opens: C:\recycler\
Opens: C:\WINDOWS\system32\uxtheme.dll

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\d0d59c2e7bbd82b1db28d7f2d0381f4c.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
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\user32.dll
Opens key: HKLM\system\currentcontrolset\control\session manager
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\imm32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mpr.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\oleaut32.dll
Opens 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\shell32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\iertutil.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\urlmon.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\normaliz.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wininet.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: HKCU\
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop
Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder
Opens key: HKLM\software\microsoft\ole
Opens key: HKCR\interface
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\microsoft\oleaut\userera
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance
Opens key: HKLM\system\setup
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
Opens key: HKCU\software\classes\
Opens key: HKCU\software\classes\protocols\name-space handler\
Opens key: HKCR\protocols\name-space handler
Opens key: HKCU\software\classes\protocols\name-space handler
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\

Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key: HKLM\system\currentcontrolset\control\wmi\security
Opens key: HKCU\software\borland\locales
Opens key: HKLM\software\borland\locales
Opens key: HKCU\software\borland\delphi\locales
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctf.dll
Opens key: HKLM\software\microsoft\ctf\compatibility\d0d59c2e7bbd82b1db28d7f2d0381f4c.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: 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: HKCU\software\webroot\window washer\paths
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows\currentversion
Opens key: HKLM\system\currentcontrolset\control\keyboard layouts\00000409
Opens key: HKCU\control panel\input method\hot keys
Opens key: HKCU\control panel\input method\hot keys\00000010
Opens key: HKCU\control panel\input method\hot keys\00000011
Opens key: HKCU\control panel\input method\hot keys\00000012
Opens key: HKCU\control panel\input method\hot keys\00000070
Opens key: HKCU\control panel\input method\hot keys\00000071
Opens key: HKCU\control panel\input method\hot keys\00000072
Opens key: HKCU\control panel\input method\hot keys\00000200
Opens key: HKCU\control panel\input method\hot keys\00000201
Opens key: HKCU\control panel\input method\hot keys\00000202
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\netscape.exe
Opens key: HKCU\software\netscape\netscape navigator\biff
Opens key: HKLM\software\netscape\netscape navigator\users
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\netscp6.exe
Opens key: HKLM\software\netscape\netscape 6
Opens key: HKLM\software\mozilla\netscape 6 \bin
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\netscp.exe
Opens key: HKLM\software\netscape\netscape
Opens key: HKLM\software\mozilla\netscape \bin
Opens key: HKLM\software\netscape\netscape navigator
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\aol.exe
Opens key: HKLM\software\america online\aol\currentversion
Opens key: HKLM\software\america online\america online\4.0
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\d0d59c2e7bbd82b1db28d7f2d0381f4c.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\system\currentcontrolset\control\computername
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKCU\software\webroot\window washer\advanced
Opens key: HKCU\software\classes\clsid\{6b38e760-d2f9-11d7-b4e1-000347126e46}\shellid

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\software\microsoft\windows nt\currentversion\image file execution options\xpsp2res.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
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\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[d0d59c2e7bbd82b1db28d7f2d0381f4c]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[d0d59c2e7bbd82b1db28d7f2d0381f4c]
Queries value: 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: 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\system\setup[systemsetupinprogress]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[disableimprovedzonecheck]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[d0d59c2e7bbd82b1db28d7f2d0381f4c.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[*]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-ab78-1084642581fb]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-0000-000000000000]
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: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[personal]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[appdata]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[local appdata]
Queries value: HKLM\system\currentcontrolset\control\keyboard layouts\00000409[layout file]
Queries value: HKLM\system\currentcontrolset\control\keyboard layouts\00000409[attributes]
Queries value: HKCU\control panel\input method\hot keys\00000010[virtual key]

Queries value: HKCU\control panel\input method\hot keys\00000010[key modifiers]
Queries value: HKCU\control panel\input method\hot keys\00000010[target ime]
Queries value: HKCU\control panel\input method\hot keys\00000011[virtual key]
Queries value: HKCU\control panel\input method\hot keys\00000011[key modifiers]
Queries value: HKCU\control panel\input method\hot keys\00000011[target ime]
Queries value: HKCU\control panel\input method\hot keys\00000012[virtual key]
Queries value: HKCU\control panel\input method\hot keys\00000012[key modifiers]
Queries value: HKCU\control panel\input method\hot keys\00000012[target ime]
Queries value: HKCU\control panel\input method\hot keys\00000070[virtual key]
Queries value: HKCU\control panel\input method\hot keys\00000070[key modifiers]
Queries value: HKCU\control panel\input method\hot keys\00000070[target ime]
Queries value: HKCU\control panel\input method\hot keys\00000071[virtual key]
Queries value: HKCU\control panel\input method\hot keys\00000071[key modifiers]
Queries value: HKCU\control panel\input method\hot keys\00000071[target ime]
Queries value: HKCU\control panel\input method\hot keys\00000072[virtual key]
Queries value: HKCU\control panel\input method\hot keys\00000072[key modifiers]
Queries value: HKCU\control panel\input method\hot keys\00000072[target ime]
Queries value: HKCU\control panel\input method\hot keys\00000200[virtual key]
Queries value: HKCU\control panel\input method\hot keys\00000200[key modifiers]
Queries value: HKCU\control panel\input method\hot keys\00000200[target ime]
Queries value: HKCU\control panel\input method\hot keys\00000201[virtual key]
Queries value: HKCU\control panel\input method\hot keys\00000201[key modifiers]
Queries value: HKCU\control panel\input method\hot keys\00000201[target ime]
Queries value: HKCU\control panel\input method\hot keys\00000202[virtual key]
Queries value: HKCU\control panel\input method\hot keys\00000202[key modifiers]
Queries value: HKCU\control panel\input method\hot keys\00000202[target ime]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[desktop]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[favorites]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[fonts]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[nethood]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[printhood]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[programs]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[sendto]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[start menu]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[startup]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[templates]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[my pictures]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[local settings]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[content]
Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir]
Queries value: HKLM\software\microsoft\windows\currentversion[mediapath]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]
Queries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
Queries value: HKCU\control panel\desktop[lamebuttontext]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[tahoma]

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