Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	1
Risk Level:	7
Date Processed:	2016-03-02 17:52:12 (UTC)
Processing Time:	62.76 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\Code_Injection_64bit.exe"
Sample ID:	1
Type:	basic
Owner:	admin
Label:	Code_Injection_64bit.exe
Date Added:	2016-03-02 17:52:11 (UTC)
File Type:	PE32:win64
File Size:	112640 bytes
MD5:	67463d13ff54e8dc7d97d43f952c36ff
SHA256:	cd06e1cdaec478f79cc4d19ab34eb4d9745d09dcdbeae5f7df647a278376f312
Description:	None

Pattern Matching Results

7	Injects thread into Windows process
4	Checks whether debugger is present
2	64 bit executable
7	Writes to memory of system processes
4	Reads process memory

Process/Thread Events

Creates process:	C:\windows\temp\Code_Injection_64bit.exe ["C:\windows\temp\Code_Injection_64bit.exe"]
Creates process:	C:\Windows\notepad.exe ["C:\Windows\notepad.exe"]
Reads from process:	PID:2956 C:\Windows\notepad.exe
Reads from process:	PID:1448 C:\Windows\SysWOW64\calc.exe
Writes to process:	PID:1120 C:\Windows\explorer.exe
Terminates process:	C:\Windows\Temp\Code_Injection_64bit.exe
Creates remote thread:	C:\Windows\explorer.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates event:	\BaseNamedObjects\ConsoleEvent-0x0000000000000B64
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

File System Events

Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\notepad.exe
Opens:	C:\Windows\AppPatch\AppPatch64\sysmain.sdb
Opens:	C:\Windows
Opens:	C:\
Opens:	C:\Windows\System32\DriverStore\FileRepository\tkbtnpn.inf_061cd165\lencins.dll
Opens:	C:\Program Files (x86)\Common Files\Microsoft Shared\Ink\mshwusa.dll
Opens:	C:\Windows\notepad.exe.Local\
Opens:	C:\Windows\winsxs\amd64_microsoft.windows.common-

```
controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9ac
  Opens:                   C:\Windows\winsxs\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9ac\comctl32.dll
  Opens:                   C:\Windows\WINSPOOL.DRV
  Opens:                   C:\Windows\System32\winspool.drv
  Opens:                   C:\Windows\VERSION.dll
  Opens:                   C:\Windows\System32\version.dll
  Opens:                   C:\Windows\WindowsShell.Manifest
  Opens:                   C:\Windows\System32\rpcss.dll
  Opens:                   C:\Windows\CRYPTBASE.dll
  Opens:                   C:\Windows\System32\cryptbase.dll
  Opens:                   C:\Windows\System32\uxtheme.dll
  Opens:                   C:\Windows\dwmapi.dll
  Opens:                   C:\Windows\System32\dwmapi.dll
  Opens:                   C:\Windows\Fonts\StaticCache.dat
  Opens:                   C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                   C:\Windows\system32\uxtheme.dll.Config
  Opens:                   C:\Windows\Fonts\lucon.ttf
  Opens:                   C:\Windows\SysWOW64\calc.exe
  Opens:                   C:\Windows\SysWOW64
  Opens:                   C:\Users\Admin\Desktop
  Reads from:              C:\Windows\Fonts\StaticCache.dat
```

Windows Registry Events

```
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options
  Opens key:               HKLM\system\currentcontrolset\control\session manager
  Opens key:               HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:               HKLM\system\currentcontrolset\control\srp\gp\dll
  Opens key:               HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:               HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:               HKCU\
  Opens key:               HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:               HKLM\software\policies\microsoft\mui\settings
  Opens key:               HKCU\software\policies\microsoft\control panel\desktop
  Opens key:               HKCU\control panel\desktop\languageconfiguration
  Opens key:               HKCU\control panel\desktop
  Opens key:               HKCU\control panel\desktop\muicached
  Opens key:               HKLM\software\microsoft\windows\currentversion\sidebyside
  Opens key:               HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:               HKLM\
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\diagnostics
  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\software\microsoft\rpc
  Opens key:               HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:               HKLM\system\setup
  Opens key:               HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:               HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\notepad.exe
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:               HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:               HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\notepad.exe
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:               HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprocserver32
  Opens key:                HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32
  Opens key:                HKLM\software\microsoft\ctf\knownclasses
  Opens key:                HKLM\software\microsoft\ole
  Opens key:                HKLM\software\microsoft\ole\tracing
  Opens key:                HKLM\software\microsoft\oleaut
  Opens key:                HKLM\software\microsoft\windows\windows error reporting\wmr
  Opens key:                HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:                HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:                HKCU\software\microsoft\notepad
  Opens key:                HKLM\software\microsoft\notepad\defaultfonts
  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 nt\currentversion\fontlink\systemlink
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
  Opens key:                HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key:                HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:                HKCU\software\classes\applications\notepad.exe
  Opens key:                HKCR\applications\notepad.exe
  Opens key:                HKCR\applications\notepad.exe\
  Opens key:                HKLM\software\microsoft\ctf\compatibility\notepad.exe
  Opens key:                HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
  Opens key:                HKLM\software\microsoft\ctf\
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                HKCU\software\classes\applications\calc.exe
  Opens key:                HKCR\applications\calc.exe
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:            HKCU\control panel\desktop[preferreduilanguages]
  Queries value:            HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  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[code_injection_64bit]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:            HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:            HKLM\system\setup[oobeinprogress]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  Queries value:            HKLM\software\policies\microsoft\sqmclient\windows[ceipenable]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
  Queries value:            HKCU\software\microsoft\windows
nt\currentversion\appcompatflags\layers[c:\windows\notepad.exe]
  Queries value:            HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}\count[{s38os404-1q43-42s2-9305-67qr0o28sp23}\grzc\pbqr_vawrpgvba_64ovg.rkr]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\compatibility32[notepad]
  Queries value:              HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:              HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:              HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:              HKCU\software\microsoft\notepad[lfescapement]
  Queries value:              HKCU\software\microsoft\notepad[lforientation]
  Queries value:              HKCU\software\microsoft\notepad[lfweight]
  Queries value:              HKCU\software\microsoft\notepad[lfitalic]
  Queries value:              HKCU\software\microsoft\notepad[lfunderline]
  Queries value:              HKCU\software\microsoft\notepad[lfstrikeout]
  Queries value:              HKCU\software\microsoft\notepad[lfcharset]
  Queries value:              HKCU\software\microsoft\notepad[lfoutprecision]
  Queries value:              HKCU\software\microsoft\notepad[lfclipprecision]
  Queries value:              HKCU\software\microsoft\notepad[lfquality]
  Queries value:              HKCU\software\microsoft\notepad[lfpitchandfamily]
  Queries value:              HKLM\software\microsoft\notepad\defaultfonts[lffacename]
  Queries value:              HKLM\software\microsoft\notepad\defaultfonts[ipointsize]
  Queries value:              HKCU\software\microsoft\notepad[lffacename]
  Queries value:              HKCU\software\microsoft\notepad[ipointsize]
  Queries value:              HKCU\software\microsoft\notepad[fwrap]
  Queries value:              HKCU\software\microsoft\notepad[statusbar]
  Queries value:              HKCU\software\microsoft\notepad[fsavewindowpositions]
  Queries value:              HKCU\software\microsoft\notepad[szheader]
  Queries value:              HKCU\software\microsoft\notepad[sztrailer]
  Queries value:              HKCU\software\microsoft\notepad[imargintop]
  Queries value:              HKCU\software\microsoft\notepad[imarginbottom]
  Queries value:              HKCU\software\microsoft\notepad[imarginleft]
  Queries value:              HKCU\software\microsoft\notepad[imarginright]
  Queries value:              HKCU\software\microsoft\notepad[iwindowposy]
  Queries value:              HKCU\software\microsoft\notepad[iwindowposx]
  Queries value:              HKCU\software\microsoft\notepad[iwindowposdx]
  Queries value:              HKCU\software\microsoft\notepad[iwindowposdy]
  Queries value:              HKCU\software\microsoft\notepad[fmle_is_broken]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:              HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
```

```
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
  Queries value:              HKCR\applications\notepad.exe[nostartpage]
  Queries value:              HKCR\applications\notepad.exe[ishostapp]
  Queries value:              HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
  Queries value:              HKLM\software\microsoft\ctf[enableanchorcontext]
  Queries value:              HKCR\applications\notepad.exe[useexecutablefortaskbargroupicon]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}\count[{s38os404-1q43-42s2-9305-67qr0o28sp23}\abgrcnq.rkr]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
  Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}\count[{s38os404-1q43-42s2-9305-67qr0o28sp23}\grzc\pbqr_vawrpgvba_64ovg.rkr]
  Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}\count[{s38os404-1q43-42s2-9305-67qr0o28sp23}\abgrcnq.rkr]
  Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}\count[hrzr_pgyfrffvba]
  Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}\count[{s38os404-1q43-42s2-9305-67qr0o28sp23}\abgrcnq.rkr]
```