Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	450005
Risk Level:	5
Date Processed:	2016-04-08 16:37:32 (UTC)
Processing Time:	61.01 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	

`"c:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe"`

Sample ID:	718
Type:	basic
Owner:	admin
Label:	62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb
Date Added:	2016-04-08 16:37:32 (UTC)
File Type:	PE32:win32:gui
File Size:	955904 bytes
MD5:	4c838f1570b3a7ff6f491e6ec1ef6895
SHA256:	62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb
Description:	None

Pattern Matching Results

`5` Possible injector

`4` Checks whether debugger is present

Process/Thread Events

Creates process:
```
C:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe
["C:\windows\temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe" ]
```

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\62DDFBF757BE511F30B6D330963C1-E2075B81.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	

`C:\Windows\Temp\62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe`

Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\apppatch\sysmain.sdb
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-

`controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985`

Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-

`controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll`

Opens:	C:\Windows\SysWOW64\msimg32.dll
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\bcryptprimitives.dll

```
Opens:                   C:\Windows\SysWOW64\cryptbase.dll
Opens:                   C:\Windows\SysWOW64\sspicli.dll
Opens:                   C:\Windows\SysWOW64\rpcrt4.dll
Opens:                   C:\Windows\SysWOW64\advapi32.dll
Opens:                   C:\Windows\SysWOW64\ole32.dll
Opens:                   C:\Windows\SysWOW64\shlwapi.dll
Opens:                   C:\Windows\SysWOW64\shell32.dll
Opens:                   C:\Windows\SysWOW64\oleaut32.dll
Opens:                   C:\Windows\SysWOW64\iertutil.dll
Opens:                   C:\Windows\SysWOW64\wininet.dll
Opens:                   C:\Windows\SysWOW64\urlmon.dll
Opens:                   C:\Windows\SysWOW64\nsi.dll
Opens:                   C:\Windows\SysWOW64\ws2_32.dll
Opens:                   C:\Windows\SysWOW64\psapi.dll
Opens:                   C:\Windows\SysWOW64\imm32.dll
Opens:                   C:\Windows\SysWOW64\msctf.dll
Opens:                   C:\Windows\WindowsShell.Manifest
Opens:                   C:\program files\qqd1eae\log.dat
```

Windows Registry Events

```
Opens key:               HKLM\software\microsoft\wow64
Opens key:               HKLM\system\currentcontrolset\control\safeboot\option
Opens key:               HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key:               HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:               HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:               HKLM\system\currentcontrolset\control\nls\customlocale
Opens key:               HKLM\system\currentcontrolset\control\nls\language
Opens key:               HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key:               HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key:               HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key:               HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key:               HKLM\software\policies\microsoft\mui\settings
Opens key:               HKCU\
Opens key:               HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key:               HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
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\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key:               HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key:               HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
Opens key:               HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key:               HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key:               HKLM\system\currentcontrolset\control\session manager
Opens key:               HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
Opens key:               HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
Opens key:               HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
Opens key:               HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
Opens key:               HKLM\
Opens key:               HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key:               HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
```

```
   Opens key:                HKLM\system\currentcontrolset\control\lsa
   Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
   Opens key:                HKLM\software\wow6432node\microsoft\ole
   Opens key:                HKLM\software\wow6432node\microsoft\ole\tracing
   Opens key:                HKLM\software\microsoft\ole\tracing
   Opens key:                HKLM\software\wow6432node\microsoft\oleaut
   Opens key:                HKCU\software\microsoft\internet explorer\main
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
   Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[empty]
   Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
   Queries value:            HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
   Queries value:            HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
   Queries value:            HKCU\control panel\desktop[preferreduilanguages]
   Queries value:            HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
   Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[]
   Queries value:            HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
   Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
   Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
   Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb.exe]
   Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
   Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[62ddfbf757be511f30b6d330963c1345e8bef0774b2baa23c901e164b0c7afbb]
   Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
   Queries value:            HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
   Queries value:            HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
   Queries value:            HKLM\software\microsoft\ole[pageallocatorusesystemheap]
   Queries value:            HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
   Queries value:            HKLM\software\microsoft\ole[aggressivemtatesting]
   Value changes:            HKCU\software\microsoft\internet explorer\main[disable script debugger]
```