Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	624
Risk Level:	1
Date Processed:	2016-04-28 13:04:16 (UTC)
Processing Time:	61.11 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\8580e85e058f7eeb06fdfe41ee2dc28c.exe"
Sample ID:	156
Type:	basic
Owner:	admin
Label:	8580e85e058f7eeb06fdfe41ee2dc28c
Date Added:	2016-04-28 12:45:06 (UTC)
File Type:	PE32:win32:gui
File Size:	233472 bytes
MD5:	8580e85e058f7eeb06fdfe41ee2dc28c
SHA256:	625081949dcfaa738c4fa7b83992b7de9ebe8f4a6fcc431f1658383d72646ca9
Description:	None

Pattern Matching Results

`1` YARA score 1

Static Events

YARA rule hit:	OLE2
YARA rule hit:	Nonexecutable

Process/Thread Events

Creates process:	C:\windows\temp\8580e85e058f7eeb06fdfe41ee2dc28c.exe

["C:\windows\temp\8580e85e058f7eeb06fdfe41ee2dc28c.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:	\Sessions\1\BaseNamedObjects\OleDfRootB37C7B164DC8C1EB
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1
Creates semaphore:	\Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP?

8580E85E058F7EEB06FDFE41EE2DC28C.EXE

File System Events

Creates:	C:\Users\Admin\AppData\Local\Temp\~DF289FBECEE0B40F8F.TMP
Opens:	C:\Windows\Prefetch\8580E85E058F7EEB06FDFE41EE2DC-77E04686.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\MSVBVM60.DLL
Opens:	C:\Windows\System32\msvbvm60.dll
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows\System32\rpcss.dll
Opens:	C:\windows\temp\CRYPTBASE.dll
Opens:	C:\Windows\System32\cryptbase.dll
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\windows\temp\8580e85e058f7eeb06fdfe41ee2dc28c.exe.cfg
Opens:	C:\windows\temp\SXS.DLL
Opens:	C:\Windows\System32\sxs.dll

```
Opens:                  C:\Windows\System32\C_932.NLS
Opens:                  C:\Windows\System32\C_949.NLS
Opens:                  C:\Windows\System32\C_950.NLS
Opens:                  C:\Windows\System32\C_936.NLS
Opens:                  C:\Windows\Fonts\sserife.fon
Opens:                  C:\windows\temp\CRYPTSP.dll
Opens:                  C:\Windows\System32\cryptsp.dll
Opens:                  C:\Windows\System32\rsaenh.dll
Opens:                  C:\windows\temp\dwmapi.dll
Opens:                  C:\Windows\System32\dwmapi.dll
Opens:                  C:\Windows\System32\en-US\user32.dll.mui
Opens:                  C:\Windows\system32\uxtheme.dll.Config
Opens:                  C:\windows\temp\8580e85e058f7eeb06fdfe41ee2dc28c.exe.Local\
Opens:                  C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
Opens:                  C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
Opens:                  C:\Windows\WindowsShell.Manifest
Opens:                  C:\Windows\Fonts\StaticCache.dat
Opens:                  C:\windows\temp\VERSION.DLL
Opens:                  C:\Windows\System32\version.dll
Opens:                  C:\Windows\Temp\8580e85e058f7eeb06fdfe41ee2dc28c.exe
Opens:                  C:\Windows
Opens:                  C:\lripl\
Reads from:             C:\Windows\Fonts\StaticCache.dat
Reads from:             C:\Windows\System32\msvbvm60.dll
```

Windows Registry Events

```
Opens key:              HKLM\system\currentcontrolset\control\session manager
Opens key:              HKLM\system\currentcontrolset\control\terminal server
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\software\microsoft\windows nt\currentversion\image file execution
options
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
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\
Opens key:              HKLM\software\microsoft\windows nt\currentversion\windows
Opens key:              HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key:              HKLM\software\microsoft\ole
Opens key:              HKLM\software\microsoft\ole\tracing
Opens key:              HKLM\software\microsoft\oleaut
Opens key:              HKLM\system\currentcontrolset\control\nls\customlocale
Opens key:              HKLM\system\currentcontrolset\control\nls\extendedlocale
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\windows error reporting\wmr
    Opens key:              HKLM\system\currentcontrolset\control\nls\codepage
    Opens key:              HKLM\software\microsoft\vba\monitors
    Opens key:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
    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\policies\microsoft\cryptography
    Opens key:              HKLM\software\microsoft\cryptography
    Opens key:              HKLM\software\microsoft\cryptography\offload
    Opens key:              HKLM\system\currentcontrolset\control\cmf\config
    Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
    Opens key:
HKLM\software\microsoft\ctf\compatibility\8580e85e058f7eeb06fdfe41ee2dc28c.exe
    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\oleaut\userera
    Opens key:              HKCU\software\policies\microsoft\control
panel\international\calendars\twodigityearmax
    Opens key:              HKCU\control panel\international\calendars\twodigityearmax
    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:              HKLM\software\microsoft\ctf\knownclasses
    Queries value:          HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
    Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
    Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
    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\image file execution
options\dllnxoptions[usefilter]
    Queries value:          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[msvbvm60.dll]
    Queries value:          HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
    Queries value:          HKLM\software\microsoft\windows
nt\currentversion\compatibility32[8580e85e058f7eeb06fdfe41ee2dc28c]
    Queries value:          HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
    Queries value:          HKLM\software\microsoft\ole[pageallocatorusesystemheap]
    Queries value:          HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
    Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
    Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
    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\windows error reporting\wmr[disable]
    Queries value:          HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
```

```
Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[932]
Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[949]
Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[950]
Queries value:              HKLM\system\currentcontrolset\control\nls\codepage[936]
Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
Queries value:              HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value:              HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value:              HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
Queries value:              HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
Queries value:              HKLM\software\microsoft\cryptography[machineguid]
Queries value:              HKLM\system\currentcontrolset\control\cmf\config[system]
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\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
Queries value:              HKLM\software\microsoft\ctf[enableanchorcontext]
```