

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 168, Task ID: 673

Task ID:	673
Risk Level:	5
Date Processed:	2016-04-28 13:05:38 (UTC)
Processing Time:	62.51 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\128e14bdd7ddf3d8f826c0cc15d75e19.exe"
Sample ID:	168
Type:	basic
Owner:	admin
Label:	128e14bdd7ddf3d8f826c0cc15d75e19
Date Added:	2016-04-28 12:45:07 (UTC)
File Type:	PE32:win32:gui
File Size:	292864 bytes
MD5:	128e14bdd7ddf3d8f826c0cc15d75e19
SHA256:	e87e80534f7422b1c1504d83759b862a122c26dc635318ef6be2f2d2836250e6
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\128e14bdd7ddf3d8f826c0cc15d75e19.exe
["C:\windows\temp\128e14bdd7ddf3d8f826c0cc15d75e19.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\MSCTF.CtfActivated.Default1

File System Events

Opens:	C:\Windows\Prefetch\128E14BDD7DDF3D8F826C0CC15D75-36672BA7.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\System32\wow64win.dll
Opens:	C:\Windows\System32\wow64cpu.dll
Opens:	C:\Windows\system32\wow64log.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\windows\temp\128e14bdd7ddf3d8f826c0cc15d75e19.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\temp\version.dll
Opens:	C:\Windows\SysWOW64\version.dll

Opens: C:\Windows\SysWOW64\apphelp.dll
 Opens: C:\Windows\AppPatch\sysmain.sdb
 Opens: C:\Windows\Temp\128e14bdd7ddf3d8f826c0cc15d75e19.exe
 Opens: C:\Windows\AppPatch\AcGenral.dll
 Opens: C:\windows\temp\UxTheme.dll
 Opens: C:\Windows\SysWOW64\uxtheme.dll
 Opens: C:\windows\temp\WINMM.dll
 Opens: C:\Windows\SysWOW64\winmm.dll
 Opens: C:\windows\temp\samcli.dll
 Opens: C:\Windows\SysWOW64\samcli.dll
 Opens: C:\windows\temp\MSACM32.dll
 Opens: C:\Windows\SysWOW64\msacm32.dll
 Opens: C:\windows\temp\sfc.dll
 Opens: C:\Windows\SysWOW64\sfc.dll
 Opens: C:\windows\temp\sfc_os.DLL
 Opens: C:\Windows\SysWOW64\sfc_os.dll
 Opens: C:\windows\temp\USERENV.dll
 Opens: C:\Windows\SysWOW64\userenv.dll
 Opens: C:\windows\temp\profapi.dll
 Opens: C:\Windows\SysWOW64\profapi.dll
 Opens: C:\windows\temp\dwmapi.dll
 Opens: C:\Windows\SysWOW64\dwmapi.dll
 Opens: C:\windows\temp\MPR.dll
 Opens: C:\Windows\SysWOW64\mpr.dll
 Opens: C:\windows\temp\128e14bdd7ddf3d8f826c0cc15d75e19.exe.Config
 Opens: C:\Windows\SysWOW64\imm32.dll
 Opens: C:\Windows\WindowsShell.Manifest
 Opens: C:\Windows\SysWOW64\en-US\setupapi.dll.mui
 Opens: C:\windows\temp\128e14bdd7ddf3d8f826c0cc15d75e19.ENU
 Opens: C:\windows\temp\128e14bdd7ddf3d8f826c0cc15d75e19.ENU.DLL
 Opens: C:\windows\temp\128e14bdd7ddf3d8f826c0cc15d75e19.EN
 Opens: C:\windows\temp\128e14bdd7ddf3d8f826c0cc15d75e19.EN.DLL
 Opens: C:\Windows\Fonts\StaticCache.dat
 Opens: C:\Windows\SysWOW64\en-US\user32.dll.mui
 Opens: C:\Windows\Temp
 Opens: C:\Windows\SysWOW64\rpcss.dll
 Opens: C:\Windows\winsxs\x86_microsoft.windows.c.-
 controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9
 Opens: C:\Windows\winsxs\x86_microsoft.windows.c.-
 controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\comctl32.dll.mui
 Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens: C:\Windows\Fonts\tahoma.ttf
 Opens: C:\Windows\Fonts\sserife.fon
 Opens: C:\Windows\SysWOW64\UxTheme.dll.Config
 Opens: C:\Windows\Fonts\msgothic.ttc
 Opens: C:\Windows\Fonts\mingliu.ttc
 Opens: C:\Windows\Fonts\simsum.ttc
 Opens: C:\Windows\Fonts\gulim.ttc
 Opens: C:\Windows\Fonts\tahomabd.ttf
 Opens: C:\windows\temp\EngSetup.dll
 Opens: C:\Windows\SysWOW64\EngSetup.dll
 Opens: C:\Windows\system\EngSetup.dll
 Opens: C:\Windows\EngSetup.dll
 Opens: C:\Windows\SysWOW64\Wbem\EngSetup.dll
 Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\EngSetup.dll
 Opens: C:\windows\temp\imageres.dll
 Opens: C:\Windows\SysWOW64\imageres.dll
 Opens: C:\Windows\SysWOW64\en-US\imageres.dll.mui
 Opens: C:\Windows\SysWOW64\ole32.dll
 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\software\microsoft\wow64
- Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file

execution options

- 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\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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots

- Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
- Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
- Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\windows file

protection

- Opens key: HKLM\software\policies\microsoft\windows nt\windows file protection
- Opens key: HKLM\
- Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\diagnostics

- 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\software\wow6432node\microsoft\windows nt\currentversion\windows
- 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: HKLM\system\currentcontrolset\services\crypt32
- Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings

- Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings

- Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings

- Opens key: HKLM\system\currentcontrolset\control\cmf\config
- Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
- Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup
- Opens key: HKLM\software\microsoft\windows\currentversion\setup
- Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion
- Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
- Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder
- Opens key: HKCU\software\borland\locales

Opens key: HKLM\software\wow6432node\borland\locales
 Opens key: HKCU\software\borland\delphi\locales
 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\wow6432node\microsoft\windows\currentversion\app
 paths\aol.exe
 Opens key: HKLM\software\microsoft\windows\currentversion\app paths\aol.exe
 Opens key: HKLM\software\wow6432node\america online\aol\currentversion
 Opens key: HKLM\software\wow6432node\america online\america online\4.0
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\app
 paths\netscape.exe
 Opens key: HKLM\software\microsoft\windows\currentversion\app paths\netscape.exe
 Opens key: HKCU\software\netscape\netscape navigator\biff
 Opens key: HKLM\software\wow6432node\netscape\netscape navigator\users
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\app
 paths\netscp6.exe
 Opens key: HKLM\software\microsoft\windows\currentversion\app paths\netscp6.exe
 Opens key: HKLM\software\wow6432node\netscape\netscape 6
 Opens key: HKLM\software\wow6432node\mozilla\netscape 6 \bin
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\app
 paths\netscp.exe
 Opens key: HKLM\software\microsoft\windows\currentversion\app paths\netscp.exe
 Opens key: HKLM\software\wow6432node\netscape\netscape
 Opens key: HKLM\software\wow6432node\mozilla\netscape \bin
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
 Opens key: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback\tahoma
 Opens key: HKLM\software\wow6432node\microsoft\ctf\compatibility\128e14bdd7ddf3d8f826c0cc15d75e19.exe
 Opens key: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\fontsubstitutes
 Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
 Opens key: HKLM\software\wow6432node\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
 0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
 Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
 0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
 Opens key: HKLM\software\wow6432node\microsoft\ctf\
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
 Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
 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\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: 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[alternatencodepage]
 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: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
 Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
 Queries value: HKLM\software\policies\microsoft\windows nt\windows file
protection[knowndlllist]
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[128e14bdd7ddf3d8f826c0cc15d75e19]
 Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
 Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
 Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]
 Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
 Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
 Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
 Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
 Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
 Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
 Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
 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
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: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[tahoma]
Queries value: HKCU\control panel\desktop[smoothscroll]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
ui]
Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]