

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 105, Task ID: 421

Task ID:	421
Risk Level:	5
Date Processed:	2016-04-28 12:58:43 (UTC)
Processing Time:	61.12 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\00a3d9dac676e47a5a3e451903adb9a8.exe"
Sample ID:	105
Type:	basic
Owner:	admin
Label:	00a3d9dac676e47a5a3e451903adb9a8
Date Added:	2016-04-28 12:45:01 (UTC)
File Type:	PE32:win32:gui
File Size:	220672 bytes
MD5:	00a3d9dac676e47a5a3e451903adb9a8
SHA256:	11fd711ff3a5a97d61d671da4cbe42ef14fc6fee479adf054a560bc0627e1897
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\00a3d9dac676e47a5a3e451903adb9a8.exe
["C:\windows\temp\00a3d9dac676e47a5a3e451903adb9a8.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\00A3D9DAC676E47A5A3E451903ADB-0F36CA5E.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\00a3d9dac676e47a5a3e451903adb9a8.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\windows\temp\00a3d9dac676e47a5a3e451903adb9a8.ENU

Opens:	C:\windows\temp\00a3d9dac676e47a5a3e451903adb9a8.ENU.DLL
Opens:	C:\windows\temp\00a3d9dac676e47a5a3e451903adb9a8.EN
Opens:	C:\windows\temp\00a3d9dac676e47a5a3e451903adb9a8.EN.DLL
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\windows\temp\dwmapl.dll
Opens:	C:\Windows\SysWOW64\dwmapl.dll
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\Windows\SysWOW64\en-US\user32.dll.mui
Opens:	C:\Windows\Temp
Opens:	C:\??\C:\windows\temp\Langs\
Opens:	C:\windows\temp\alcoholx.dll
Opens:	C:\Windows\SysWOW64\alcoholx.dll
Opens:	C:\Windows\system\alcoholx.dll
Opens:	C:\Windows\alcoholx.dll
Opens:	C:\Windows\SysWOW64\Wbem\alcoholx.dll
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\alcoholx.dll
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\SysWOW64\rpcss.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Reads from:	C:\Windows\Fonts\StaticCache.dat

Windows Registry Events

Creates key:	HKCU\software\alcohol soft\alcohol 120%\
Creates key:	HKCU\software
Creates key:	HKCU\software\alcohol soft
Creates key:	HKCU\software\alcohol soft\alcohol 120%
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:	HKLM\system\currentcontrolset\control\nls\sorting\versions
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: 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\extendedlocale
  Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  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\system\currentcontrolset\control\cmf\config
  Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\alcohol.exe
  Opens key: HKLM\software\microsoft\windows\currentversion\app paths\alcohol.exe
  Opens key: HKCU\software\alcohol soft\alcohol 120%\options
  Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\00a3d9dac676e47a5a3e451903adb9a8.exe
  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\
  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[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: 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[00a3d9dac676e47a5a3e451903adb9a8]
  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\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
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\system\currentcontrolset\control\cmf\config[system]
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]