

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 105, Task ID: 419

Task ID:	419
Risk Level:	5
Date Processed:	2016-04-28 12:58:14 (UTC)
Processing Time:	61.08 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:	\BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.IMG
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.AP
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.AP.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceiveConection.Event.AP.IC
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Opens:	C:\WINDOWS\Prefetch\00A3D9DAC676E47A5A3E451903ADB-0D573973.pf
Opens:	C:\Documents and Settings\Admin

Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\system32\comctl32.dll
Opens:	C:\WINDOWS\system32\COMCTL32.DLL.124.Manifest
Opens:	C:\WINDOWS\system32\COMCTL32.DLL.124.Config
Opens:	C:\WINDOWS\system32\shell32.dll
Opens:	C:\WINDOWS\system32\SHELL32.DLL.124.Manifest
Opens:	C:\WINDOWS\system32\SHELL32.DLL.124.Config
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens:	C:\WINDOWS\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config
Opens:	C:\WINDOWS\system32\MSCTF.dll
Opens:	C:\WINDOWS\system32\MSCTFIME.IME
Opens:	C:\WINDOWS\Temp
Opens:	C:\??\c:\windows\temp\Langs\

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\00a3d9dac676e47a5a3e451903adb9a8.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key:	HKLM\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\user32.dll
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdi32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll
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: HKCU\
 Opens key: HKCU\software\policies\microsoft\control panel\desktop
 Opens key: HKCU\control panel\desktop
 Opens key: HKLM\software\microsoft\ole
 Opens key: HKCR\interface
 Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
 Opens key: HKLM\software\microsoft\oleaut
 Opens key: HKLM\software\microsoft\oleaut\userera
 Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance
 Opens key: HKLM\system\setup
 Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
 Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
 Opens key: HKCU\software\borland\locales
 Opens key: HKLM\software\borland\locales
 Opens key: HKCU\software\borland\delphi\locales
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\msctf.dll
 Opens key: HKLM\software\microsoft\ctf\compatibility\00a3d9dac676e47a5a3e451903adb9a8.exe
 Opens key: HKLM\software\microsoft\ctf\systemshared\
 Opens key: HKCU\keyboard layout\toggle
 Opens key: HKLM\software\microsoft\ctf\
 Opens key: HKLM\software\microsoft\windows nt\currentversion\imm
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\version.dll
 Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\msctfime.ime
 Opens key: HKCU\software\microsoft\ctf
 Opens key: HKLM\software\microsoft\ctf\systemshared
 Opens key: HKLM\software\microsoft\windows\currentversion\app paths\alcohol.exe
 Opens key: HKCU\software\alcohol soft\alcohol 120%\options
 Opens key: HKCU\software\microsoft\ctf\langbaraddin\
 Opens key: HKLM\software\microsoft\ctf\langbaraddin\
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\compatibility32[00a3d9dac676e47a5a3e451903adb9a8]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
 compatibility[00a3d9dac676e47a5a3e451903adb9a8]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
 Queries value: HKCU\control panel\desktop[multiulanguageid]
 Queries value: HKCU\control panel\desktop[smoothscroll]
 Queries value: HKLM\system\currentcontrolset\control\session
 manager[criticalsectiontimeout]
 Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]
 Queries value: HKCR\interface[interfacehelperdisableall]
 Queries value: HKCR\interface[interfacehelperdisableallforole32]
 Queries value: HKCR\interface[interfacehelperdisabletypelib]
 Queries value: HKCR\interface\{00020400-0000-0000-c000-
 000000000046}[interfacehelperdisableall]

Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableallforole32]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKLM\software\microsoft\ctf\systemshared[cuas]
Queries value: HKCU\keyboard layout\toggle[language hotkey]
Queries value: HKCU\keyboard layout\toggle[hotkey]
Queries value: HKCU\keyboard layout\toggle[layout hotkey]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]