

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 108, Task ID: 431

Task ID:	431
Risk Level:	1
Date Processed:	2016-04-28 12:58:47 (UTC)
Processing Time:	62.17 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\890e1107c5fb51e6d819558f4036ba22.exe"
Sample ID:	108
Type:	basic
Owner:	admin
Label:	890e1107c5fb51e6d819558f4036ba22
Date Added:	2016-04-28 12:45:01 (UTC)
File Type:	PE32:win32:gui
File Size:	675840 bytes
MD5:	890e1107c5fb51e6d819558f4036ba22
SHA256:	1a58bb0f53d25d4e4f796820aa7eb8139c5201eeb8849cba3d324f467e3fcb5
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\890e1107c5fb51e6d819558f4036ba22.exe
["c:\windows\temp\890e1107c5fb51e6d819558f4036ba22.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:	\BaseNamedObjects\MSCTF.Shared.MUTEX.IK
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.AJC
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.AJC.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceiveConection.Event.AJC.IC
Creates semaphore:	\BaseNamedObjects\C:\?WINDOWS?TEMP?890E1107C5FB51E6D819558F4036BA22.EXE
Creates semaphore:	\BaseNamedObjects\OleDfRoot000021545

File System Events

Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\~DF1548.tmp
Opens:	C:\WINDOWS\Prefetch\890E1107C5FB51E6D819558F4036B-238BB4E6.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\msvbvm60.dll

Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\system32\rpcss.dll
Opens:	C:\WINDOWS\system32\MSCTF.dll
Opens:	C:\WINDOWS\system32\sxs.dll
Opens:	C:\WINDOWS\system32\MSCTFIME.IME
Opens:	C:\WINDOWS\system32\clbcatq.dll
Opens:	C:\WINDOWS\system32\comres.dll
Opens:	C:\WINDOWS\Registration\R0000000000007.clb
Opens:	C:\WINDOWS\Fonts\sserife.fon
Reads from:	C:\WINDOWS\Registration\R0000000000007.clb

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\890e1107c5fb51e6d819558f4036ba22.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
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\gdi32.dll
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\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\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\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\msvbvm60.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:	HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key:	HKLM\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\diagnostics
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:	HKCU\
Opens key:	HKCU\software\policies\microsoft\control panel\desktop
Opens key:	HKCU\control panel\desktop
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctf.dll
Opens key:	

HKLM\software\microsoft\ctf\compatibility\890e1107c5fb51e6d819558f4036ba22.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\image file execution
options\sxs.dll
 Opens key: HKLM\system\setup
 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\system\currentcontrolset\control\nls\codepage
 Opens key: HKLM\software\microsoft\vba\monitors
 Opens key: HKLM\software\microsoft\com3
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comres.dll
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\clbcatq.dll
 Opens key: HKLM\software\microsoft\com3\debug
 Opens key: HKCU\software\classes\
 Opens key: HKLM\software\classes
 Opens key: HKU\
 Opens key: HKCR\clsid
 Opens key: HKCU\software\classes\clsid\{7a6325e1-f655-41cc-b13b-ab1a54ae1d3c}
 Opens key: HKCR\clsid\{7a6325e1-f655-41cc-b13b-ab1a54ae1d3c}
 Opens key: HKCU\software\classes\clsid\{35053a22-8589-11d1-b16a-00c0f0283628}
 Opens key: HKCR\clsid\{35053a22-8589-11d1-b16a-00c0f0283628}
 Opens key: HKCU\software\policies\microsoft\windows\app management
 Opens key: HKLM\software\policies\microsoft\windows\app management
 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\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[890e1107c5fb51e6d819558f4036ba22]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[890e1107c5fb51e6d819558f4036ba22]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
 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[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: HKCU\control panel\desktop[multiuilanguageid]
 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\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
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\com3[com+enabled]
Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
Queries value: HKLM\software\microsoft\com3[regdbversion]
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]