

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 24, Task ID: 96

Task ID:	96
Risk Level:	5
Date Processed:	2016-04-28 12:49:02 (UTC)
Processing Time:	3.63 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\3d9a2ec042f97b86cf02fa354ba1414d.exe"
Sample ID:	24
Type:	basic
Owner:	admin
Label:	3d9a2ec042f97b86cf02fa354ba1414d
Date Added:	2016-04-28 12:44:52 (UTC)
File Type:	PE32:win32:gui
File Size:	45056 bytes
MD5:	3d9a2ec042f97b86cf02fa354ba1414d
SHA256:	c4e23a6b058dea1117941098c2090cab10503baa730f895eae2e10a259e3c5c6
Description:	None

Pattern Matching Results

5 Accesses Filesystem keys

Process/Thread Events

Creates process:	C:\windows\temp\3d9a2ec042f97b86cf02fa354ba1414d.exe
["C:\windows\temp\3d9a2ec042f97b86cf02fa354ba1414d.exe"]	
Terminates process:	C:\Windows\Temp\3d9a2ec042f97b86cf02fa354ba1414d.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates event:	\Security\LSA_AUTHENTICATION_INITIALIZED

File System Events

Opens:	C:\Windows\Prefetch\3D9A2EC042F97B86CF02FA354BA14-77F94D92.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\apphelp.dll
Opens:	C:\Windows\AppPatch\sysmain.sdb
Opens:	C:\Windows\Temp\3d9a2ec042f97b86cf02fa354ba1414d.exe
Opens:	C:\Windows\AppPatch\AcSpecfc.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\windows\temp\3d9a2ec042f97b86cf02fa354ba1414d.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\temp\mscms.dll
Opens:	C:\Windows\SysWOW64\mscms.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\WINMM.dll

Opens:	C:\Windows\SysWOW64\winmm.dll
Opens:	C:\windows\temp\DDRAW.dll
Opens:	C:\Windows\SysWOW64\ddraw.dll
Opens:	C:\windows\temp\DCIMAN32.dll
Opens:	C:\Windows\SysWOW64\dciman32.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\msi.dll
Opens:	C:\Windows\SysWOW64\msi.dll
Opens:	C:\Windows\AppPatch\AcLayers.dll
Opens:	C:\windows\temp\WINSPOOL.DRV
Opens:	C:\Windows\SysWOW64\winspool.drv
Opens:	C:\Windows\AppPatch\AcGenral.dll
Opens:	C:\windows\temp\UxTheme.dll
Opens:	C:\Windows\SysWOW64\uxtheme.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\VERSION.dll
Opens:	C:\Windows\SysWOW64\version.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\3d9a2ec042f97b86cf02fa354ba1414d.exe.Manifest
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\en-US\setupapi.dll.mui

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\system\currentcontrolset\control\nls\sorting\versions
Opens key:	HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key:	

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
 Opens key: HKLM\
 Opens key: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\diagnostics
 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\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\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\software\policies\microsoft\sqmclient\windows
 Opens key: HKLM\software\microsoft\sqmclient\windows
 Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder
 Opens key: HKLM\system\currentcontrolset\control\filesystem
 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\software\wow6432node\microsoft\rpc
 Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
 Opens key: HKLM\system\setup
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
 Opens key: HKLM\software\policies\microsoft\windows nt\rpc
 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: HKCU\software\microsoft\windows
 nt\currentversion\appcompatflags[showdebuginfo]
 Queries value: HKLM\software\policies\microsoft\windows nt\windows file
 protection[knowndlllist]

Queries value: HKLM\software\microsoft\windows
 nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\compatibility32[3d9a2ec042f97b86cf02fa354ba1414d]
 Queries value: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\windows[loadappinit_dlls]
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value: HKLM\system\currentcontrolset\control\wmi\security[d53270e3-c8cf-4707-
 958a-dad20c90073c]
 Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
 Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]
 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\software\microsoft\sqmclient\windows[ceipenable]
 Queries value: HKLM\system\currentcontrolset\control\filesystem[win31filesystem]
 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\software\microsoft\rpc[maxrpcsize]
 Queries value:
 HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
 Queries value: HKLM\system\setup[oobeinprogress]
 Queries value: HKLM\system\setup[systemsetupinprogress]