

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 45, Task ID: 179

Task ID:	179
Risk Level:	5
Date Processed:	2016-04-28 12:52:02 (UTC)
Processing Time:	61.14 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9db0cad36abcee711515983a365920b2.exe"
Sample ID:	45
Type:	basic
Owner:	admin
Label:	9db0cad36abcee711515983a365920b2
Date Added:	2016-04-28 12:44:54 (UTC)
File Type:	PE32:win32:gui
File Size:	721694 bytes
MD5:	9db0cad36abcee711515983a365920b2
SHA256:	e3d049d927d38e962579f15ef74c2fa4f7c92afdccfb60e13221ed2b505d656e
Description:	None

## Pattern Matching Results

- 5 Resource section contains an executable
- 2 64 bit executable
- 5 Possible injector

## Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Resource section contains an executable

## Process/Thread Events

Creates process:	C:\windows\temp\9db0cad36abcee711515983a365920b2.exe
["C:\windows\temp\9db0cad36abcee711515983a365920b2.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\9DB0CAD36ABCEE711515983A36592-28F3823A.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\mpr.dll
Opens:	C:\Windows\System32\mpr.dll
Opens:	C:\windows\temp\version.dll
Opens:	C:\Windows\System32\version.dll
Opens:	C:\windows\temp\9db0cad36abcee711515983a365920b2.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\System32\imm32.dll
Opens:	C:\Windows\WindowsShell.Manifest
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\windows\temp\dwmapi.dll

Opens:	C:\Windows\System32\dwmapi.dll
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\Windows\System32\en-US\user32.dll.mui
Opens:	C:\Windows\System32\rpcss.dll
Opens:	C:\windows\temp\CRYPTBASE.dll
Opens:	C:\Windows\System32\cryptbase.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows\System32\en-US\KernelBase.dll.mui
Opens:	C:\windows\temp\netmsg.dll
Opens:	C:\Windows\System32\netmsg.dll
Opens:	C:\Windows\System32\en-US\netmsg.dll.mui
Opens:	C:\Windows\Temp\9db0cad36abcee711515983a365920b2.exe
Opens:	C:\windows\temp\9db0cad36abcee711515983a365920b2.dat
Opens:	C:\windows\temp\imageres.dll
Opens:	C:\Windows\System32\imageres.dll
Opens:	C:\Windows\System32\en-US\imageres.dll.mui
Reads from:	C:\Windows\Fonts\StaticCache.dat
Reads from:	C:\Windows\Temp\9db0cad36abcee711515983a365920b2.exe

## Windows Registry Events

---

Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\ddl
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\
Opens key:	HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key:	HKLM\software\policies\microsoft\mui\settings
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\microsoft\windows\currentversion\sidebyside
Opens key:	HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key:	HKLM\system\currentcontrolset\control\nls\sorting\versions
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\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\windows
Opens key:	HKLM\software\microsoft\ole
Opens key:	HKLM\software\microsoft\ole\tracing
Opens key:	HKLM\software\microsoft\oleaut
Opens key:	HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key:	HKLM\system\currentcontrolset\control\networkprovider\hworder
Opens key:	HKLM\software\microsoft\windows\windows error reporting\wmr
Opens key:	HKLM\system\currentcontrolset\control\nls\customlocale
Opens key:	HKLM\system\currentcontrolset\control\nls\extendedlocale
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\microsoft\ctf\compatibility\9db0cad36abcee711515983a365920b2.exe  
Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}  
Opens key: HKLM\software\microsoft\ctf\  
Opens key: HKLM\software\microsoft\ctf\knownclasses  
Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer  
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer  
Queries value: HKLM\system\currentcontrolset\control\session  
manager[cwdillegalindllsearch]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]  
Queries value: HKCU\control panel\desktop[preferreduilanguages]  
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]  
Queries value: HKLM\system\currentcontrolset\control\ntp\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\microsoft\windows  
nt\currentversion\compatibility32[9db0cad36abcee711515983a365920b2]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\windows[loadappinit\_dlls]  
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]  
Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]  
Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]  
Queries value: HKLM\system\currentcontrolset\control\ntp\customlocale[en-us]  
Queries value: HKLM\system\currentcontrolset\control\ntp\extendedlocale[en-us]  
Queries value: HKLM\system\currentcontrolset\control\ntp\locale[00000409]  
Queries value: HKLM\system\currentcontrolset\control\ntp\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\microsoft\ctf[enableanchorcontext]