

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 137, Task ID: 548

Task ID:	548
Risk Level:	1
Date Processed:	2016-04-28 13:01:58 (UTC)
Processing Time:	61.11 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9b4d5407eec5e669a16910215b954cb8.exe"
Sample ID:	137
Type:	basic
Owner:	admin
Label:	9b4d5407eec5e669a16910215b954cb8
Date Added:	2016-04-28 12:45:04 (UTC)
File Type:	PE32:win32:gui
File Size:	340776 bytes
MD5:	9b4d5407eec5e669a16910215b954cb8
SHA256:	eb6dcb3f3f2189b1fe35b7822050729fc22a00ec3b48c39173895d6a8144a4fd
Description:	None

## Pattern Matching Results

### Process/Thread Events

Creates process:	C:\windows\temp\9b4d5407eec5e669a16910215b954cb8.exe
["C:\windows\temp\9b4d5407eec5e669a16910215b954cb8.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\9B4D5407EEC5E669A16910215B954-623A1966.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\WSOCK32.dll
Opens:	C:\Windows\System32\wsock32.dll
Opens:	C:\windows\temp\9b4d5407eec5e669a16910215b954cb8.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\System32\sechost.dll
Opens:	C:\windows\temp\WINSPOOL.DRV
Opens:	C:\Windows\System32\winspool.drv
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\windows\temp\dwmapl.dll
Opens:	C:\Windows\System32\dwmapl.dll
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\Windows\System32\en-US\user32.dll.mui
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\windows\temp\urlswmr.txt
Opens:	C:\
Opens:	C:\Windows\Fonts\sserife.fon
Opens:	C:\windows\temp\RICHED32.DLL
Opens:	C:\Windows\System32\riched32.dll
Opens:	C:\windows\temp\RICHED20.dll
Opens:	C:\Windows\System32\riched20.dll
Opens:	C:\Windows\win.ini
Opens:	C:\Windows\System32\rpcss.dll
Opens:	C:\windows\temp\CRYPTBASE.dll
Opens:	C:\Windows\System32\cryptbase.dll
Opens:	C:\Windows\System32\mswsock.dll
Opens:	C:\Windows\System32\WSH_TCPIP.DLL
Reads from:	C:\Windows\Fonts\StaticCache.dat
Reads from:	C:\Windows\win.ini

### Windows Registry Events

Creates key:	HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms
Creates key:	HKCU\software\microsoft\netshow\player\general
Creates key:	HKCU\software
Creates key:	HKCU\software\microsoft
Creates key:	HKCU\software\microsoft\netshow
Creates key:	HKCU\software\microsoft\netshow\player
Creates key:	HKCU\software\microsoft\netshow\player\local

Opens key: HKLM\system\currentcontrolset\control\session manager  
Opens key: HKLM\system\currentcontrolset\control\terminal server  
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\ntp\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\windows nt\currentversion\diagnostics  
Opens key: HKLM\software\microsoft\ole  
Opens key: HKLM\software\microsoft\ole\tracing  
Opens key: HKLM\software\microsoft\oleaut  
Opens key: HKLM\system\currentcontrolset\services\crypt32  
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings  
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet  
settings  
Opens key: HKLM\system\currentcontrolset\control\ntp\customlocale  
Opens key: HKLM\system\currentcontrolset\control\ntp\extendedlocale  
Opens key: HKLM\system\currentcontrolset\control\ntp\locale  
Opens key: HKLM\system\currentcontrolset\control\ntp\locale\alternate sorts  
Opens key: HKLM\system\currentcontrolset\control\ntp\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\policies\microsoft\sqlclient\windows  
Opens key: HKLM\software\microsoft\sqlclient\windows  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\07e9109d  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\000000019  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000001  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000002  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000003  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000005  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000006  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000007  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000008  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000009  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000010  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000011  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000012  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000013

Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000014  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000015  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000016  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000017  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000018  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\0000000c  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000002  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006  
Opens key: HKCU\software\microsoft\windows nt\currentversion\windows  
Opens key:  
HKLM\software\microsoft\ctf\compatibility\9b4d5407eec5e669a16910215b954cb8.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\system\currentcontrolset\services\winsock\parameters  
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock  
Opens key: HKLM\system\currentcontrolset\services\psched\parameters\winsock  
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers  
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\psched  
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock  
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip  
Opens key: HKCU\software\microsoft\mediaplayer\preferences  
Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\http  
Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms  
Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\rtsp  
Opens key: HKCU\software\microsoft\netshow\player\general  
Opens key: HKCU\software\microsoft\netshow\player\local  
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: 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\locale\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\microsoft\windows  
nt\currentversion\compatibility32[9b4d5407eec5e669a16910215b954cb8]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\windows[loadappinit\_dlls]  
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]  
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheapisprivate]  
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[disableimprovedzonecheck]  
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet  
settings[security\_hklm\_only]  
Queries value: HKLM\system\currentcontrolset\control\locale\nls\customlocale[en-us]  
Queries value: HKLM\system\currentcontrolset\control\locale\nls\extendedlocale[en-us]  
Queries value: HKLM\system\currentcontrolset\control\locale\nls\locale[00000409]  
Queries value: HKLM\system\currentcontrolset\control\locale\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]

[illegible]

[illegible]

Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[enabled]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[version]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[storsserviceclassinfo]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerinfo]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[librarypath]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[displaystring]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerid]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[addressfamily]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[supportednamespace]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[enabled]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[version]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[storsserviceclassinfo]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerinfo]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2\_32numhandlebuckets]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2\_32spincount]  
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]  
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]  
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]  
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrollldelay]  
Queries value: HKCU\software\microsoft\windows  
nt\currentversion\windows[scrollinterval]  
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]  
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]  
Queries value:  
HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]  
Queries value: HKLM\system\currentcontrolset\services\winsock\setup  
migration\providers\psched[winsock 2.0 provider id]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]  
Queries value: HKLM\system\currentcontrolset\services\winsock\setup  
migration\providers\tcpip[winsock 2.0 provider id]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]  
Sets/Creates value: HKCU\software\microsoft\mediaplayer\preferences[usehttp]  
Sets/Creates value: HKCU\software\microsoft\mediaplayer\preferences[usetcp]  
Sets/Creates value: HKCU\software\microsoft\mediaplayer\preferences[useudp]  
Sets/Creates value: HKCU\software\microsoft\mediaplayer\preferences[usemulticast]  
Sets/Creates value:  
HKCU\software\microsoft\mediaplayer\preferences\proxysettings\http[proxyhost]  
Sets/Creates value:  
HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms[proxyport]  
Sets/Creates value:  
HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms[proxystyle]  
Sets/Creates value:  
HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms[proxybypass]  
Sets/Creates value:  
HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms[proxyname]  
Sets/Creates value:  
HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms[proxyhost]  
Sets/Creates value:  
HKCU\software\microsoft\mediaplayer\preferences\proxysettings\rtsp[proxyhost]  
Sets/Creates value: HKCU\software\microsoft\netshow\player\general[enablehttp]  
Sets/Creates value: HKCU\software\microsoft\netshow\player\general[enabletcp]  
Sets/Creates value: HKCU\software\microsoft\netshow\player\general[enableudp]  
Sets/Creates value: HKCU\software\microsoft\netshow\player\general[enablemulticast]  
Sets/Creates value: HKCU\software\microsoft\netshow\player\general[firstprotocol]  
Sets/Creates value: HKCU\software\microsoft\netshow\player\local[appliedautoproxy]  
Sets/Creates value: HKCU\software\microsoft\netshow\player\local[enableautoproxy]  
Sets/Creates value: HKCU\software\microsoft\netshow\player\local[proxyenabled]

Sets/Creates value: HKCU\software\microsoft\netshow\player\local[proxyname]  
Sets/Creates value: HKCU\software\microsoft\netshow\player\local[proxyhost]  
Sets/Creates value: HKCU\software\microsoft\netshow\player\local[proxyport]  
Value changes:  
HKCU\software\microsoft\mediaplayer\preferences\proxysettings\http[proxyport]  
Value changes:  
HKCU\software\microsoft\mediaplayer\preferences\proxysettings\http[proxystyle]  
Value changes:  
HKCU\software\microsoft\mediaplayer\preferences\proxysettings\http[proxybypass]  
Value changes:  
HKCU\software\microsoft\mediaplayer\preferences\proxysettings\http[proxyname]  
Value changes:  
HKCU\software\microsoft\mediaplayer\preferences\proxysettings\rtsp[proxyport]  
Value changes:  
HKCU\software\microsoft\mediaplayer\preferences\proxysettings\rtsp[proxystyle]  
Value changes:  
HKCU\software\microsoft\mediaplayer\preferences\proxysettings\rtsp[proxybypass]  
Value changes:  
HKCU\software\microsoft\mediaplayer\preferences\proxysettings\rtsp[proxyname]