

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 3318, Task ID: 781

Task ID:	781
Risk Level:	10
Date Processed:	2016-05-18 10:37:41 (UTC)
Processing Time:	61.99 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\f0da8593d29e9b367fda7028db12cab0.exe"
Sample ID:	3318
Type:	basic
Owner:	admin
Label:	f0da8593d29e9b367fda7028db12cab0
Date Added:	2016-05-18 10:30:50 (UTC)
File Type:	PE32:win32:gui
File Size:	323584 bytes
MD5:	f0da8593d29e9b367fda7028db12cab0
SHA256:	08257c7a15283c59cc8cd4e76c326b009fac61607d7c9d1def559b41b079f8ce
Description:	None

## Pattern Matching Results

- 5 PE: Contains compressed section
- 3 Program causes a crash [Info]
- 10 Creates malicious mutex: QQLogger [Backdoor, keylogger]

## Process/Thread Events

Creates process: C:\windows\temp\f0da8593d29e9b367fda7028db12cab0.exe  
["C:\windows\temp\f0da8593d29e9b367fda7028db12cab0.exe" ]

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex  
Creates mutex: \Sessions\1\BaseNamedObjects\setup\_fat32sys  
Creates event: \KernelObjects\SystemErrorPortReady

## File System Events

Opens: C:\Windows\Prefetch\F0DA8593D29E9B367FDA7028DB12C-9B78E492.pf  
Opens: C:\Windows\System32  
Opens: C:\Windows\System32\sechost.dll  
Opens: C:\Windows\System32\apphelp.dll  
Opens: C:\Windows\AppPatch\sysmain.sdb  
Opens: C:\Windows\Temp\f0da8593d29e9b367fda7028db12cab0.exe  
Opens: C:\Windows\AppPatch\AcGenral.dll  
Opens: C:\windows\temp\SspiCli.dll  
Opens: C:\Windows\System32\sspicli.dll  
Opens: C:\windows\temp\UxTheme.dll  
Opens: C:\Windows\System32\uxtheme.dll  
Opens: C:\windows\temp\WINMM.dll  
Opens: C:\Windows\System32\winmm.dll  
Opens: C:\windows\temp\samcli.dll  
Opens: C:\Windows\System32\samcli.dll  
Opens: C:\windows\temp\MSACM32.dll  
Opens: C:\Windows\System32\msacm32.dll  
Opens: C:\windows\temp\VERSION.dll  
Opens: C:\Windows\System32\version.dll  
Opens: C:\windows\temp\sfc.dll  
Opens: C:\Windows\System32\sfc.dll  
Opens: C:\windows\temp\sfc\_os.DLL

Opens:	C:\Windows\System32\sfc_os.dll
Opens:	C:\windows\temp\USERENV.dll
Opens:	C:\Windows\System32\userenv.dll
Opens:	C:\windows\temp\profapi.dll
Opens:	C:\Windows\System32\profapi.dll
Opens:	C:\windows\temp\dwmapi.dll
Opens:	C:\Windows\System32\dwmapi.dll
Opens:	C:\windows\temp\MPR.dll
Opens:	C:\Windows\System32\mpr.dll
Opens:	C:\windows\temp\f0da8593d29e9b367fda7028db12cab0.exe.Manifest
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\System32\en-US\setupapi.dll.mui
Opens:	C:\Users\Admin\AppData\Local\Temp\MSAPI.DAT
Reads from:	C:\Windows\Temp\f0da8593d29e9b367fda7028db12cab0.exe

## Windows Registry Events

Deletes value:	HKLM\system\currentcontrolset\control\session
manager[pendingfilerenameoperations]	
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\dll
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:	HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key:	HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key:	HKLM\software\policies\microsoft\windows nt\windows file protection
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\control\cmf\config
Opens key:	HKLM\software\microsoft\windows\windows error reporting\wmr
Opens key:	HKLM\software\microsoft\windows\currentversion\setup
Opens key:	HKLM\software\microsoft\windows\currentversion
Opens key:	HKLM\system\currentcontrolset\control\nls\customlocale
Opens key:	HKLM\system\currentcontrolset\control\nls\extendedlocale
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\networkprovider\hworder
Opens key:	HKLM\software\microsoft\windows\currentversion\explorer\shell folders
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: HKCU\software\microsoft\windows  
nt\currentversion\appcompatflags[showdebuginfo]  
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]  
Queries value: HKLM\software\policies\microsoft\windows nt\windows file  
protection[knowndlllist]  
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[f0da8593d29e9b367fda7028db12cab0]  
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\system\currentcontrolset\control\cmf\config[system]  
Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]  
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]  
Queries value: HKLM\software\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\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\software\microsoft\windows\currentversion\explorer\shell  
folders[common appdata]