

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 622, Task ID: 2435

Task ID:	2435
Risk Level:	1
Date Processed:	2016-02-22 05:29:44 (UTC)
Processing Time:	3.81 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe"
Sample ID:	622
Type:	basic
Owner:	admin
Label:	33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99
Date Added:	2016-02-22 05:26:49 (UTC)
File Type:	PE32:win32:gui
File Size:	54272 bytes
MD5:	75984f5cee7f9e64b9ffe44f60df8764
SHA256:	33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99
Description:	None

## Pattern Matching Results

## Process/Thread Events

Creates process:	C:\windows\temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe
	["C:\windows\temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe" ]
Terminates process:	C:\Windows\Temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe

## Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObje
----------------	---------------------------

## File System Events

Opens:	C:\Windows\Prefetch\33A18D17F6F150459E8EB2593A364-EB28559C.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.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\System32\imm32.dll
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\windows\temp\dwmapi.dll
Opens:	C:\Windows\System32\dwmapi.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls

## Windows Registry Events

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\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\windows nt\currentversion\diagnostics  
 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  
 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\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[33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99]  
 Queries value: HKLM\software\microsoft\windows  
 nt\currentversion\windows[loadappinit\_dlls]  
 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\control\nls\locale[00000409]  
 Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]