Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 194, Task ID: 775

Task ID:	775
Risk Level:	4
Date Processed:	2016-04-28 13:08:45 (UTC)
Processing Time:	2.15 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\319835aa5f0566aab8efd7630e010b78.exe"
Sample ID:	194
Type:	basic
Owner:	admin
Label:	319835aa5f0566aab8efd7630e010b78
Date Added:	2016-04-28 12:45:10 (UTC)
File Type:	PE32:win32:gui
File Size:	84776 bytes
MD5:	319835aa5f0566aab8efd7630e010b78
SHA256:	9d60256b3184049d9c80b3c5df3d807d632fde34515123cbfdfd784875f13141
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\319835aa5f0566aab8efd7630e010b78.exe ["c:\windows\temp\319835aa5f0566aab8efd7630e010b78.exe"]
Terminates process:	C:\WINDOWS\Temp\319835aa5f0566aab8efd7630e010b78.exe

Named Object Events

Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Opens:	C:\WINDOWS\Prefetch\319835AA5F0566AAB8EFD7630E010-36D8696E.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\system32\urlmon.dll.123.Manifest
Opens:	C:\WINDOWS\system32\urlmon.dll.123.Config
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens:	C:\WINDOWS\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config
Opens:	C:\WINDOWS\system32\WININET.dll.123.Manifest
Opens:	C:\WINDOWS\system32\WININET.dll.123.Config

Windows Registry Events

Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\319835aa5f0566aab8efd7630e010b78.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution

```
options\rpcrt4.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\winlogon
  Opens key:               HKLM\
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll
  Opens key:               HKLM\system\currentcontrolset\control\session manager
  Opens key:               HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:               HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:               HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\normaliz.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iertutil.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\urlmon.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wininet.dll
  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\software\microsoft\windows nt\currentversion\windows
  Opens key:               HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key:               HKLM\software\microsoft\ole
  Opens key:               HKCR\interface
  Opens key:               HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:               HKLM\software\microsoft\oleaut
  Opens key:               HKLM\software\microsoft\oleaut\userera
  Opens key:               HKCU\
  Opens key:               HKCU\software\policies\microsoft\control panel\desktop
  Opens key:               HKCU\control panel\desktop
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\languagepack
  Opens key:               HKCU\software\classes\
  Opens key:               HKCU\software\classes\protocols\name-space handler\
  Opens key:               HKCR\protocols\name-space handler
  Opens key:               HKCU\software\classes\protocols\name-space handler
  Opens key:               HKCU\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:               HKLM\software\microsoft\windows\currentversion\internet settings
  Opens key:               HKLM\software\policies\microsoft\windows\currentversion\internet
```

```
settings
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
  Opens key:                HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKLM\software\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:                HKLM\system\currentcontrolset\control\wmi\security
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[319835aa5f0566aab8efd7630e010b78]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[319835aa5f0566aab8efd7630e010b78]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
  Queries value:            HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Queries value:            HKCR\interface[interfacehelperdisableall]
  Queries value:            HKCR\interface[interfacehelperdisableallforole32]
  Queries value:            HKCR\interface[interfacehelperdisabletypelib]
  Queries value:            HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
  Queries value:            HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
  Queries value:            HKCU\control panel\desktop[multiuilanguageid]
  Queries value:            HKCU\control panel\desktop[smoothscroll]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[319835aa5f0566aab8efd7630e010b78.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
  Queries value:            HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]
  Queries value:            HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
```

0000-000000000000]

Value changes: HKLM\software\microsoft\cryptography\rng[seed]