Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 67, Task ID: 268

Task ID:	268
Risk Level:	4
Date Processed:	2016-04-28 12:54:15 (UTC)
Processing Time:	2.45 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\1e8f8a944f52914954a311162a0dca29.exe"

Sample ID:	67
Type:	basic
Owner:	admin
Label:	1e8f8a944f52914954a311162a0dca29
Date Added:	2016-04-28 12:44:56 (UTC)
File Type:	PE32:win32:gui
File Size:	316264 bytes
MD5:	1e8f8a944f52914954a311162a0dca29
SHA256:	0dc07f2b3ae9116c6ed41a81a94826071fcbeb44774d4ffe703de3f3e51061b8
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\1e8f8a944f52914954a311162a0dca29.exe ["C:\windows\temp\1e8f8a944f52914954a311162a0dca29.exe"]
Terminates process:	C:\Windows\Temp\1e8f8a944f52914954a311162a0dca29.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\BaseNamedObjects\1e8f8a944f52914954a311162a0dca29LogMutex

File System Events

Opens:	C:\Windows\Prefetch\1E8F8A944F52914954A311162A0DC-AB260FCA.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\1e8f8a944f52914954a311162a0dca29.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\imm32.dll
Opens:	C:\Windows\System32\rpcss.dll
Opens:	C:\windows\temp\CRYPTBASE.dll
Opens:	C:\Windows\System32\cryptbase.dll
Opens:	C:\Windows\System32\uxtheme.dll

Windows Registry Events

Creates key:	HKCU\software\appdatalow\software\plus-hd-2.4\log
Creates key:	HKCU\software
Creates key:	HKCU\software\appdatalow
Creates key:	HKCU\software\appdatalow\software
Creates key:	HKCU\software\appdatalow\software\plus-hd-2.4
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:
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\software\microsoft\ole
  Opens key:               HKLM\software\microsoft\ole\tracing
  Opens key:               HKLM\software\microsoft\oleaut
  Opens key:               HKCU\software\appdatalow\software\plus-hd-2.4\log
  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\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[1e8f8a944f52914954a311162a0dca29]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:           HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:           HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:           HKCU\software\appdatalow\software\plus-hd-
2.4\log[1e8f8a944f52914954a311162a0dca29]
  Sets/Creates value:      HKCU\software\appdatalow\software\plus-hd-
2.4\log[1e8f8a944f52914954a311162a0dca29]
```