Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 182, Task ID: 728

Task ID:	728
Risk Level:	5
Date Processed:	2016-04-28 13:07:37 (UTC)
Processing Time:	2.45 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\25f7bf77d10cdb430f1cff51671d34fd.exe"
Sample ID:	182
Type:	basic
Owner:	admin
Label:	25f7bf77d10cdb430f1cff51671d34fd
Date Added:	2016-04-28 12:45:08 (UTC)
File Type:	PE32:win32:gui
File Size:	51200 bytes
MD5:	25f7bf77d10cdb430f1cff51671d34fd
SHA256:	4ca2f583d836280ec408acd86d807826e975cb14bb82852c6c5009f7aec9e56e
Description:	None

Pattern Matching Results

2	PE: Nonstandard section
5	Packer: UPX
5	PE: Contains compressed section

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX

Process/Thread Events

Creates process:	C:\windows\temp\25f7bf77d10cdb430f1cff51671d34fd.exe ["C:\windows\temp\25f7bf77d10cdb430f1cff51671d34fd.exe"]
Terminates process:	C:\Windows\Temp\25f7bf77d10cdb430f1cff51671d34fd.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\25F7BF77D10CDB430F1CFF51671D3-CDE8993A.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\25f7bf77d10cdb430f1cff51671d34fd.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\temp\25f7bf77d10cdb430f1cff51671d34fd.ENU
Opens:	C:\windows\temp\25f7bf77d10cdb430f1cff51671d34fd.ENU.DLL
Opens:	C:\windows\temp\25f7bf77d10cdb430f1cff51671d34fd.EN
Opens:	C:\windows\temp\25f7bf77d10cdb430f1cff51671d34fd.EN.DLL

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\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\
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\diagnostics
  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\ole
  Opens key:               HKLM\software\microsoft\ole\tracing
  Opens key:               HKLM\software\microsoft\oleaut
  Opens key:               HKCU\software\borland\locales
  Opens key:               HKLM\software\borland\locales
  Opens key:               HKCU\software\borland\delphi\locales
  Opens key:               HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:               HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:               HKLM\software\microsoft\windows\windows error reporting\wmr
  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[25f7bf77d10cdb430f1cff51671d34fd]
  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:           HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:           HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:           HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
```