Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 8, Task ID: 31

Task ID:	31
Risk Level:	1
Date Processed:	2016-04-28 12:46:47 (UTC)
Processing Time:	2.52 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	`"c:\windows\temp\839732664a17eb4effe85e010e105500.exe"`

Sample ID:	8
Type:	basic
Owner:	admin
Label:	839732664a17eb4effe85e010e105500
Date Added:	2016-04-28 12:44:50 (UTC)
File Type:	PE32:win32:gui
File Size:	46424 bytes
MD5:	839732664a17eb4effe85e010e105500
SHA256:	5171fb029a69b2e42a3720b1587aa210cbd72628c0894a6e1dd3662acaa060f2
Description:	None

Pattern Matching Results

Static Events

Anomaly:	`PE: Contains a virtual section`

Process/Thread Events

Creates process:	`C:\windows\temp\839732664a17eb4effe85e010e105500.exe ["C:\windows\temp\839732664a17eb4effe85e010e105500.exe" ]`
Terminates process:	`C:\Windows\Temp\839732664a17eb4effe85e010e105500.exe`

Named Object Events

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

File System Events

Opens:	`C:\Windows\Prefetch\839732664A17EB4EFFE85E010E105-84B9D68D.pf`
Opens:	`C:\Windows\System32`
Opens:	`C:\Windows\System32\sechost.dll`
Opens:	`C:\Windows\System32\imm32.dll`
Opens:	`C:\windows\temp\839732664a17eb4effe85e010e105500.ENU`
Opens:	`C:\windows\temp\839732664a17eb4effe85e010e105500.ENU.DLL`
Opens:	`C:\windows\temp\839732664a17eb4effe85e010e105500.EN`
Opens:	`C:\windows\temp\839732664a17eb4effe85e010e105500.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\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\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[839732664a17eb4effe85e010e105500]
  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]
```