Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 194, Task ID: 776

Task ID:	776
Risk Level:	4
Date Processed:	2016-04-28 13:08:45 (UTC)
Processing Time:	2.45 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 mutex:	`\Sessions\1\BaseNamedObjects\DBWinMutex`

File System Events

Opens:	`C:\Windows\Prefetch\319835AA5F0566AAB8EFD7630E010-A6E2A67D.pf`
Opens:	`C:\Windows\System32`
Opens:	`C:\Windows\System32\sechost.dll`
Opens:	`C:\Windows\System32\imm32.dll`

Windows Registry Events

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\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:                HKLM\system\currentcontrolset\services\crypt32
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet settings
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings
  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[319835aa5f0566aab8efd7630e010b78]
  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\services\crypt32[debugheapflags]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
  Queries value:            HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
```