Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 87, Task ID: 349

Task ID:	349
Risk Level:	4
Date Processed:	2016-04-28 12:56:36 (UTC)
Processing Time:	3.07 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9051f3a2023c56661804fd664e27c74c.exe"

Sample ID:	87
Type:	basic
Owner:	admin
Label:	9051f3a2023c56661804fd664e27c74c
Date Added:	2016-04-28 12:44:59 (UTC)
File Type:	PE32:win32:gui
File Size:	312320 bytes
MD5:	9051f3a2023c56661804fd664e27c74c
SHA256:	8ac177e931c1a04d468ba07162f5acdf48cbb1e1351afbbbf6ca99dac795e079
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\9051f3a2023c56661804fd664e27c74c.exe ["C:\windows\temp\9051f3a2023c56661804fd664e27c74c.exe"]
Terminates process:	C:\Windows\Temp\9051f3a2023c56661804fd664e27c74c.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\9051F3A2023C56661804FD664E27C-FC80E9F4.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\System32\wow64win.dll
Opens:	C:\Windows\System32\wow64cpu.dll
Opens:	C:\Windows\system32\wow64log.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\windows\temp\IPHLPAPI.DLL
Opens:	C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens:	C:\windows\temp\WINNSI.DLL
Opens:	C:\Windows\SysWOW64\winnsi.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\windows\temp\MSVCP100.dll
Opens:	C:\Windows\SysWOW64\msvcp100.dll
Opens:	C:\windows\temp\MSVCR100.dll
Opens:	C:\Windows\SysWOW64\msvcr100.dll
Opens:	C:\windows\temp\VERSION.dll
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\windows\temp\WINHTTP.dll
Opens:	C:\Windows\SysWOW64\winhttp.dll
Opens:	C:\windows\temp\webio.dll
Opens:	C:\Windows\SysWOW64\webio.dll
Opens:	C:\Windows\SysWOW64\imm32.dll

Windows Registry Events

```
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options
  Opens key:              HKLM\system\currentcontrolset\control\session manager
  Opens key:              HKLM\software\microsoft\wow64
  Opens key:              HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
  Opens key:              HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:              HKLM\system\currentcontrolset\control\srp\gp\dll
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:              HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:              HKLM\system\currentcontrolset\control\nls\language
  Opens key:              HKLM\system\currentcontrolset\control\mui\uilanguages
  Opens key:              HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
  Opens key:              HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
  Opens key:              HKLM\software\wow6432node\policies\microsoft\mui\settings
  Opens key:              HKLM\software\policies\microsoft\mui\settings
  Opens key:              HKCU\
  Opens key:              HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:              HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
  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\wow6432node\microsoft\windows\currentversion\sidebyside
  Opens key:              HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:              HKLM\
  Opens key:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
  Opens key:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
  Opens key:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
  Opens key:              HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
  Opens key:              HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  Opens key:              HKLM\software\wow6432node\microsoft\ole
  Opens key:              HKLM\software\wow6432node\microsoft\ole\tracing
  Opens key:              HKLM\software\microsoft\ole\tracing
  Opens key:              HKLM\software\wow6432node\microsoft\oleaut
  Opens key:              HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  Opens key:              HKCU\software\classes\
  Opens key:              HKCU\software\classes\appid
  Opens key:              HKCR\appid
  Opens key:              HKCU\software\classes\appid\{068808b5-8e5c-463b-97ec-548be3668d1d}
  Opens key:              HKCR\appid\{068808b5-8e5c-463b-97ec-548be3668d1d}
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
  Queries value:          HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[empty]
  Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
  Queries value:          HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
  Queries value:          HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
  Queries value:          HKCU\control panel\desktop[preferreduilanguages]
  Queries value:              HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\wow6432node\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\wow6432node\microsoft\windows
nt\currentversion\compatibility32[9051f3a2023c56661804fd664e27c74c]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:              HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:              HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
```