Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	800
Risk Level:	4
Date Processed:	2016-04-28 13:09:41 (UTC)
Processing Time:	2.63 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\c09c9e59db51bb2921c8c38799359a80.exe"

Sample ID:	200
Type:	basic
Owner:	admin
Label:	c09c9e59db51bb2921c8c38799359a80
Date Added:	2016-04-28 12:45:10 (UTC)
File Type:	PE32:win32:gui
File Size:	196624 bytes
MD5:	c09c9e59db51bb2921c8c38799359a80
SHA256:	a39590aa899aded009b14b66c435ea14d1362c20bb6cc0c577c05ac7a6fa9a07
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\c09c9e59db51bb2921c8c38799359a80.exe ["C:\windows\temp\c09c9e59db51bb2921c8c38799359a80.exe"]
Terminates process:	C:\Windows\Temp\c09c9e59db51bb2921c8c38799359a80.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\C09C9E59DB51BB2921C8C38799359-CC619175.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\rpc
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\system\setup
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                HKLM\software\microsoft\sqmclient\windows
  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[c09c9e59db51bb2921c8c38799359a80]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:            HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:            HKLM\system\setup[oobeinprogress]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  Queries value:            HKLM\software\microsoft\sqmclient\windows[ceipenable]
```