Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	731
Risk Level:	6
Date Processed:	2016-05-18 10:31:20 (UTC)
Processing Time:	61.6 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\35644f3d0029f81c3d478d3c2407fac3.exe"
Sample ID:	3306
Type:	basic
Owner:	admin
Label:	35644f3d0029f81c3d478d3c2407fac3
Date Added:	2016-05-18 10:30:48 (UTC)
File Type:	PE32:win32:gui
File Size:	597504 bytes
MD5:	35644f3d0029f81c3d478d3c2407fac3
SHA256:	05093ba493e460b909f4922656c72a340517b31d8d6ff569dd73a2c1c9fc04dd
Description:	None

Pattern Matching Results

`2` PE: Nonstandard section
`6` Suspicious packer: VMProtect

Static Events

Anomaly:	PE: Contains one or more non-standard sections

Process/Thread Events

Creates process:	C:\windows\temp\35644f3d0029f81c3d478d3c2407fac3.exe

["C:\windows\temp\35644f3d0029f81c3d478d3c2407fac3.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\35644F3D0029F81C3D478D3C2407F-83FCDD92.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\35644f3d0029f81c3d478d3c2407fac3.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\apppatch\sysmain.sdb
Opens:	C:\Windows\SysWOW64\netapi32.dll
Opens:	C:\Windows\SysWOW64\pdh.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\netutils.dll
Opens:	C:\Windows\SysWOW64\srvcli.dll
Opens:	C:\Windows\SysWOW64\wkscli.dll
Opens:	C:\Windows\SysWOW64\SHCore.dll
Opens:	C:\Windows\SysWOW64\combase.dll

Windows Registry Events

```
   Opens key:                     HKLM\software\microsoft\wow64
   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\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
   Opens key:                     HKCU\software\microsoft\windows nt\currentversion\appcompatflags
   Opens key:                     HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
   Opens key:                     HKLM\system\currentcontrolset\control\session manager
   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:                 HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
   Queries value:                 HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
```