Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	386
Risk Level:	7
Date Processed:	2016-04-28 12:57:41 (UTC)
Processing Time:	61.07 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\e55165a67c552497d9d653069eae0a8c.exe"
Sample ID:	97
Type:	basic
Owner:	admin
Label:	e55165a67c552497d9d653069eae0a8c
Date Added:	2016-04-28 12:45:00 (UTC)
File Type:	PE32:win32:gui
File Size:	110080 bytes
MD5:	e55165a67c552497d9d653069eae0a8c
SHA256:	e30c0a5cd916b4f9242e6d77470cff238914cd16806422a8c4f422b37976aa6b
Description:	None

Pattern Matching Results

`7` YARA score 7

Static Events

YARA rule hit:	KeyLoggerStrings

Process/Thread Events

Creates process:	C:\windows\temp\e55165a67c552497d9d653069eae0a8c.exe

["C:\windows\temp\e55165a67c552497d9d653069eae0a8c.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\E55165A67C552497D9D653069EAE0-329CDBF9.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\e55165a67c552497d9d653069eae0a8c.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

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]
```