# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

| | |
|---|---|
| Task ID: | 448 |
| Risk Level: | 5 |
| Date Processed: | 2016-04-28 12:59:19 (UTC) |
| Processing Time: | 61.16 seconds |
| Virtual Environment: | IntelliVM |
| Execution Arguments: | "c:\windows\temp\71c1e0867f9e956b63caf58170d6e3eb.exe" |
| | |
| Sample ID: | 112 |
| Type: | basic |
| Owner: | admin |
| Label: | 71c1e0867f9e956b63caf58170d6e3eb |
| Date Added: | 2016-04-28 12:45:01 (UTC) |
| File Type: | PE32:win32:gui |
| File Size: | 142336 bytes |
| MD5: | 71c1e0867f9e956b63caf58170d6e3eb |
| SHA256: | 156e8d7c52b44144528f838bd44b9e6eff6ea09078e2aa0059353038d7033764 |
| Description: | None |

## Pattern Matching Results

`4` Checks whether debugger is present
`5` Accesses Filesystem keys

## Process/Thread Events

| | |
|---|---|
| Creates process: | C:\windows\temp\71c1e0867f9e956b63caf58170d6e3eb.exe |

["C:\windows\temp\71c1e0867f9e956b63caf58170d6e3eb.exe" ]

## Named Object Events

| | |
|---|---|
| Creates mutex: | \Sessions\1\BaseNamedObjects\DBWinMutex |
| Creates mutex: | \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0 |
| Creates mutex: | \Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1 |
| Creates event: | \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1 |

## File System Events

| | |
|---|---|
| Opens: | C:\Windows\Prefetch\71C1E0867F9E956B63CAF58170D6E-1D440361.pf |
| Opens: | C:\Windows\System32 |
| Opens: | C:\windows\temp\msi.dll |
| Opens: | C:\Windows\System32\msi.dll |
| Opens: | C:\Windows\System32\sechost.dll |
| Opens: | C:\Windows\System32\imm32.dll |
| Opens: | C:\Windows\Fonts\StaticCache.dat |
| Opens: | C:\Windows\System32\uxtheme.dll |
| Opens: | C:\windows\temp\dwmapi.dll |
| Opens: | C:\Windows\System32\dwmapi.dll |
| Opens: | C:\Windows\System32\rpcss.dll |
| Opens: | C:\windows\temp\CRYPTBASE.dll |
| Opens: | C:\Windows\System32\cryptbase.dll |
| Opens: | C:\Windows\Globalization\Sorting\SortDefault.nls |
| Reads from: | C:\Windows\Fonts\StaticCache.dat |

## 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\system\currentcontrolset\control\filesystem
  Opens key:            HKLM\software\microsoft\windows\currentversion\installer\userdata\s-1-5-
21-2160590473-689474908-1361669368-1002\components\6c3c47cd8bac94c4eb81b5d1dcd091e7
  Opens key:            HKLM\software\microsoft\windows\currentversion\installer\userdata\s-1-5-
18\components\6c3c47cd8bac94c4eb81b5d1dcd091e7
  Opens key:            HKLM\software\microsoft\windows\windows error reporting\wmr
  Opens key:            HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:            HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:            HKLM\system\currentcontrolset\control\nls\locale
  Opens key:            HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
  Opens key:            HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:            HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
  Opens key:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
  Opens key:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
  Opens key:            HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
  Opens key:
HKLM\software\microsoft\ctf\compatibility\71c1e0867f9e956b63caf58170d6e3eb.exe
  Opens key:            HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
  Opens key:            HKLM\software\microsoft\ctf\
  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[71c1e0867f9e956b63caf58170d6e3eb]
  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\control\filesystem[win31filesystem]
  Queries value:       HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
```

Queries value:                HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value:                HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value:                HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value:                HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
Queries value:                HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
Queries value:                HKLM\software\microsoft\ctf[enableanchorcontext]