Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	801
Risk Level:	2
Date Processed:	2016-05-18 10:40:01 (UTC)
Processing Time:	8.34 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\0f8136b03b3fe3078d8f97f99eb96ccd.exe"
Sample ID:	3323
Type:	basic
Owner:	admin
Label:	0f8136b03b3fe3078d8f97f99eb96ccd
Date Added:	2016-05-18 10:30:50 (UTC)
File Type:	PE32:win32:gui
File Size:	165384 bytes
MD5:	0f8136b03b3fe3078d8f97f99eb96ccd
SHA256:	70973762204438d307467456e3690ae67a69ebd57e6a7e54fac990b32a6fbfa1
Description:	None

Pattern Matching Results

`2` PE: Nonstandard section

Static Events

Anomaly:	PE: No DOS stub
Anomaly:	PE: Contains one or more non-standard sections

Process/Thread Events

Creates process:	C:\windows\temp\0f8136b03b3fe3078d8f97f99eb96ccd.exe

["C:\windows\temp\0f8136b03b3fe3078d8f97f99eb96ccd.exe"]

Terminates process:	C:\Windows\Temp\0f8136b03b3fe3078d8f97f99eb96ccd.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates event:	\KernelObjects\MaximumCommitCondition
Creates event:	\Security\LSA_AUTHENTICATION_INITIALIZED

File System Events

Creates:	C:\ProgramData\Mozilla
Creates:	C:\ProgramData\Mozilla\puqlymm.exe
Opens:	C:\Windows\Prefetch\0F8136B03B3FE3078D8F97F99EB96-DBCD7A71.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\ulib.dll
Opens:	C:\Windows\System32\ulib.dll
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\System32\rpcss.dll
Opens:	C:\windows\temp\CRYPTBASE.dll
Opens:	C:\Windows\System32\cryptbase.dll
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\windows\temp\dwmapi.dll
Opens:	C:\Windows\System32\dwmapi.dll
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\ProgramData\Mozilla
Opens:	C:\
Opens:	C:\Windows\Temp\0f8136b03b3fe3078d8f97f99eb96ccd.exe

```
Opens:                   C:\Windows\System32\taskschd.dll
Opens:                   C:\windows\temp\SspiCli.dll
Opens:                   C:\Windows\System32\sspicli.dll
Opens:                   C:\windows\temp\XmlLite.dll
Opens:                   C:\Windows\System32\xmllite.dll
Writes to:               C:\ProgramData\Mozilla\puqlymm.exe
Reads from:              C:\Windows\Fonts\StaticCache.dat
Reads from:              C:\Windows\Temp\0f8136b03b3fe3078d8f97f99eb96ccd.exe
```

Windows Registry Events

```
Opens key:               HKLM\system\currentcontrolset\control\session manager
Opens key:               HKLM\system\currentcontrolset\control\terminal server
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\
Opens key:               HKLM\system\currentcontrolset\services\crypt32
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\software\microsoft\windows nt\currentversion\windows
Opens key:               HKLM\software\microsoft\ole
Opens key:               HKLM\software\microsoft\ole\tracing
Opens key:               HKLM\software\microsoft\windows nt\currentversion\diagnostics
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\oleaut
Opens key:               HKLM\software\microsoft\windows\windows error reporting\wmr
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\windows\currentversion\explorer\shell folders
Opens key:               HKLM\software\microsoft\cryptography
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
Opens key:               HKCU\software\classes\
Opens key:               HKCU\software\classes\appid\0f8136b03b3fe3078d8f97f99eb96ccd.exe
Opens key:               HKCR\appid\0f8136b03b3fe3078d8f97f99eb96ccd.exe
Opens key:               HKLM\system\currentcontrolset\control\lsa
Opens key:               HKLM\software\microsoft\com3
```

```
Opens key:              HKCU\software\classes\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}
Opens key:              HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}
Opens key:              HKCU\software\classes\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}\treatas
Opens key:              HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\treatas
Opens key:              HKCU\software\classes\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}\progid
Opens key:              HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\progid
Opens key:              HKCU\software\classes\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}\inprocserver32
Opens key:              HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32
Opens key:              HKCU\software\classes\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}\inprochandler32
Opens key:              HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprochandler32
Opens key:              HKCU\software\classes\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}\inprochandler
Opens key:              HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprochandler
Opens key:              HKLM\system\currentcontrolset\control\computername
Queries value:          HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
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\services\crypt32[debugheapflags]
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[0f8136b03b3fe3078d8f97f99eb96ccd]
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\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\windows error reporting\wmr[disable]
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\windows\currentversion\explorer\shell
folders[common appdata]
  Queries value:            HKLM\software\microsoft\cryptography[machineguid]
  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]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value:            HKLM\software\microsoft\com3[com+enabled]
  Queries value:            HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\progid[]
  Queries value:            HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}[]
  Queries value:            HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32[]
  Queries value:            HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\microsoft\ole[maxsxshashcount]
```