Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 98, Task ID: 393

Task ID:	393
Risk Level:	4
Date Processed:	2016-04-28 12:57:45 (UTC)
Processing Time:	61.2 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\a8e55ca7e9168cd0df56a0907a3f0832.exe"

Sample ID:	98
Type:	basic
Owner:	admin
Label:	a8e55ca7e9168cd0df56a0907a3f0832
Date Added:	2016-04-28 12:45:00 (UTC)
File Type:	PE32:win32:gui
File Size:	351232 bytes
MD5:	a8e55ca7e9168cd0df56a0907a3f0832
SHA256:	64673dbcdc33f12f759be72ac47fc39a16ffe29d75c078054f37e4e85b23f82b
Description:	None

Pattern Matching Results

3 Long sleep detected
4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\a8e55ca7e9168cd0df56a0907a3f0832.exe ["C:\windows\temp\a8e55ca7e9168cd0df56a0907a3f0832.exe"]

Named Object Events

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

File System Events

Opens:	C:\Windows\Prefetch\A8E55CA7E9168CD0DF56A0907A3F0-009BEC80.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\System32\wow64win.dll
Opens:	C:\Windows\System32\wow64cpu.dll
Opens:	C:\Windows\system32\wow64log.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\windows\temp\a8e55ca7e9168cd0df56a0907a3f0832.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.vc90.atl_1fc8b3b9a1e18e3b_9.0.30729.4148_none_51ca66a2bbe76806
Opens:	C:\Windows\winsxs\x86_microsoft.vc90.atl_1fc8b3b9a1e18e3b_9.0.30729.4148_none_51ca66a2bbe76806\ATL90.dll
Opens:	C:\Windows\winsxs\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742
Opens:	C:\Windows\winsxs\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742\msvcp90.dll
Opens:	C:\Windows\winsxs\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742\msvcr90.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\
Opens:	C:\Windows\SysWOW64\rpcss.dll
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\windows\temp\CRYPTSP.dll
Opens:	C:\Windows\SysWOW64\cryptsp.dll
Opens:	C:\Windows\SysWOW64\rsaenh.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\windows\temp\RpcRtRemote.dll
Opens:	C:\Windows\SysWOW64\RpcRtRemote.dll

Windows Registry Events

```
  Creates key:              HKCU\software\samsung\kies2.0
  Creates key:              HKCU\software
  Creates key:              HKCU\software\samsung
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options
  Opens key:                HKLM\system\currentcontrolset\control\session manager
  Opens key:                HKLM\software\microsoft\wow64
  Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
  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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:                HKLM\
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
  Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
  Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  Opens key:                HKLM\software\wow6432node\microsoft\ole
  Opens key:                HKLM\software\wow6432node\microsoft\ole\tracing
  Opens key:                HKLM\software\microsoft\ole\tracing
  Opens key:                HKLM\software\wow6432node\microsoft\oleaut
  Opens key:                HKCU\software\classes\
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKCU\software\classes\wow6432node\clsid\{e0241b79-ab3a-49d8-9691-
2cf3d6d863b0}
  Opens key:                HKCR\wow6432node\clsid\{e0241b79-ab3a-49d8-9691-2cf3d6d863b0}
  Opens key:                HKCU\software\classes\clsid\{e0241b79-ab3a-49d8-9691-2cf3d6d863b0}
  Opens key:                HKCR\clsid\{e0241b79-ab3a-49d8-9691-2cf3d6d863b0}
  Opens key:                HKLM\software\wow6432node\microsoft\rpc
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\system\setup
  Opens key:                HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
  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\appid\a8e55ca7e9168cd0df56a0907a3f0832.exe
  Opens key:                HKCR\appid\a8e55ca7e9168cd0df56a0907a3f0832.exe
  Opens key:                HKLM\software\wow6432node\microsoft\ole\appcompat
  Opens key:                HKLM\software\microsoft\ole\appcompat
  Opens key:                 HKLM\system\currentcontrolset\control\lsa
  Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider
  Opens key:                 HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  Opens key:                 HKLM\software\policies\microsoft\cryptography
  Opens key:                 HKLM\software\microsoft\cryptography
  Opens key:                 HKLM\software\wow6432node\microsoft\cryptography\offload
  Opens key:                 HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}
  Opens key:                 HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
  Opens key:                 HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                 HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                 HKLM\software\wow6432node\microsoft\rpc\extensions
  Opens key:                 HKLM\software\microsoft\rpc\extensions
  Opens key:                 HKLM\system\currentcontrolset\services\bfe
  Opens key:                 HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
  Opens key:                 HKLM\software\microsoft\sqmclient\windows\disabledsessions\
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
  Queries value:             HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  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:             HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:             HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[a8e55ca7e9168cd0df56a0907a3f0832]
  Queries value:             HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:             HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:             HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:             HKCU\software\samsung\kies2.0[loglevel]
  Queries value:             HKLM\software\microsoft\com3[com+enabled]
  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\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
  Queries value:             HKLM\software\microsoft\ole[defaultaccesspermission]
  Queries value:             HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[image path]
  Queries value:             HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:             HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:              HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value:              HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
  Queries value:              HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
  Queries value:              HKLM\software\microsoft\cryptography[machineguid]
  Queries value:              HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32[]
  Queries value:              HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:              HKLM\software\microsoft\rpc\extensions[remoterpcdll]
  Queries value:              HKLM\software\microsoft\sqmclient\windows\disabledprocesses[68ab44cc]
  Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
  Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
  Queries value:              HKLM\software\microsoft\ole[maxsxshashcount]
```