Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 64, Task ID: 254

Task ID:	254
Risk Level:	1
Date Processed:	2016-04-28 12:54:07 (UTC)
Processing Time:	61.1 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9605ec58da0d3fdca8679abd4c481cc3.exe"
Sample ID:	64
Type:	basic
Owner:	admin
Label:	9605ec58da0d3fdca8679abd4c481cc3
Date Added:	2016-04-28 12:44:56 (UTC)
File Type:	PE32:win32:gui
File Size:	670328 bytes
MD5:	9605ec58da0d3fdca8679abd4c481cc3
SHA256:	6b8823f2765c3edb6cb59698c7a251607ba2db93a45594f3ce44d141bced75a9
Description:	None

Pattern Matching Results

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\windows\temp\9605ec58da0d3fdca8679abd4c481cc3.exe ["C:\windows\temp\9605ec58da0d3fdca8679abd4c481cc3.exe"]

Creates process: C:\Users\Admin\AppData\Local\Temp\is-OTRHH.tmp\9605ec58da0d3fdca8679abd4c481cc3.tmp ["C:\Users\Admin\AppData\Local\Temp\is-OTRHH.tmp\9605ec58da0d3fdca8679abd4c481cc3.tmp" /SL5="$601F2,267059,117248,C:\windows\temp\9605ec58da0d3fdca8679abd4c481cc3.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Creates: C:\Users\Admin\AppData\Local\Temp\is-OTRHH.tmp

Creates: C:\Users\Admin\AppData\Local\Temp\is-OTRHH.tmp\9605ec58da0d3fdca8679abd4c481cc3.tmp

Opens: C:\Windows\Prefetch\9605EC58DA0D3FDCA8679ABD4C481-93076565.pf

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll

Opens: C:\Windows\SysWOW64

Opens: C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985

Opens: C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll

Opens: C:\Windows\SysWOW64\sechost.dll

Opens: C:\Windows\SysWOW64\ole32.dll

Opens: C:\Windows\SysWOW64\imm32.dll

Opens: C:\Windows\WindowsShell.Manifest

Opens: C:\Windows\SysWOW64\netmsg.dll

Opens: C:\Windows\Temp\9605ec58da0d3fdca8679abd4c481cc3.exe

Opens: C:\Windows\Globalization\Sorting\SortDefault.nls

Opens: C:\Windows\SysWOW64\uxtheme.dll

Opens: C:\Windows\SysWOW64\dwmapi.dll
Opens: C:\Users\Admin\AppData\Local\Temp\is-OTRHH.tmp\9605ec58da0d3fdca8679abd4c481cc3.tmp
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\apppatch\sysmain.sdb
Opens: C:\Users\Admin\AppData\Local\Temp\is-OTRHH.tmp
Opens: C:\
Opens: C:\Users
Opens: C:\Users\Admin
Opens: C:\Users\Admin\AppData
Opens: C:\Users\Admin\AppData\Local
Opens: C:\Users\Admin\AppData\Local\Temp
Opens: C:\Windows\Prefetch\9605EC58DA0D3FDCA8679ABD4C481-DF39E7E7.pf
Opens: C:\Windows\SysWOW64\msimg32.dll
Opens: C:\Windows\SysWOW64\version.dll
Opens: C:\Windows\SysWOW64\mpr.dll
Opens: C:\Windows\SysWOW64\SHCore.dll
Opens: C:\Windows\Fonts\tahoma.ttf
Opens: C:\Windows\Fonts\StaticCache.dat
Opens: C:\Windows\SysWOW64\uxtheme.dll.Config
Opens: C:\Windows\WinSxS\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.9200.16384_en-us_9f44aa25b2ac1b72
Opens: C:\Windows\WinSxS\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.9200.16384_en-us_9f44aa25b2ac1b72\comctl32.dll.mui
Writes to: C:\Users\Admin\AppData\Local\Temp\is-OTRHH.tmp\9605ec58da0d3fdca8679abd4c481cc3.tmp
Reads from: C:\Windows\Temp\9605ec58da0d3fdca8679abd4c481cc3.exe
Reads from: C:\Users\Admin\AppData\Local\Temp\is-OTRHH.tmp\9605ec58da0d3fdca8679abd4c481cc3.tmp
Reads from: C:\Windows\Fonts\StaticCache.dat

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\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions
Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\control\lsa

Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\
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: 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: HKCU\software\codegear\locales
Opens key: HKLM\software\wow6432node\codegear\locales
Opens key: HKCU\software\borland\locales
Opens key: HKCU\software\borland\delphi\locales
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids
Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\9605ec58da0d3fdca8679abd4c481cc3.tmp
Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\appcompat
Opens key: HKLM\software\policies\microsoft\windows\appcompat
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\9605ec58da0d3fdca8679abd4c481cc3.tmp
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\fontsubstitutes
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
Opens key: HKLM\system\currentcontrolset\control\keyboard layouts\04090409
Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\9605ec58da0d3fdca8679abd4c481cc3.tmp
Opens key: HKLM\software\wow6432node\microsoft\ctf\
Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses
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\tahoma
Opens key: HKCU\software\microsoft\windows\currentversion\uninstall\{da34b67a-29a4-
4ac2-bac5-640c1327b3e4}}_is1
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\{da34b67a-29a4-4ac2-bac5-
640c1327b3e4}}_is1

Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
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\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[9605ec58da0d3fdca8679abd4c481cc3.exe]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[9605ec58da0d3fdca8679abd4c481cc3]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags[{a9f603c2-b224-4a07-b6ea-a2bcc1a51297}]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[{a9f603c2-b224-4a07-b6ea-a2bcc1a51297}]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags[{35bf919e-0495-48df-8e74-456384e34e74}]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[{35bf919e-0495-48df-8e74-456384e34e74}]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags[{6b39d1b2-7883-4648-94bf-bd5109b4ac48}]
Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[{6b39d1b2-7883-4648-94bf-bd5109b4ac48}]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[9605ec58da0d3fdca8679abd4c481cc3.tmp]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg 2]
Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
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\windows\currentversion\policies\explorer[turnoffspianimations]