# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 175, Task ID: 698

| | |
|---|---|
| Task ID: | 698 |
| Risk Level: | 8 |
| Date Processed: | 2016-04-28 13:06:31 (UTC) |
| Processing Time: | 3.5 seconds |
| Virtual Environment: | IntelliVM |
| Execution Arguments: | "c:\windows\temp\5a9758fb7e97e044db5cf7a786ad5d7e.exe" |
| | |
| Sample ID: | 175 |
| Type: | basic |
| Owner: | admin |
| Label: | 5a9758fb7e97e044db5cf7a786ad5d7e |
| Date Added: | 2016-04-28 12:45:08 (UTC) |
| File Type: | PE32:win32:gui |
| File Size: | 717080 bytes |
| MD5: | 5a9758fb7e97e044db5cf7a786ad5d7e |
| SHA256: | 00233b7523919542345159 41d9b1a2fd32753d9c8e03203e107c7c0e09141752 |
| Description: | None |

## Pattern Matching Results

3 Writes to a log file [Info]
8 Contains suspicious Microsoft certificate
4 Reads process memory
4 Checks whether debugger is present

## Process/Thread Events

Creates process: C:\windows\temp\5a9758fb7e97e044db5cf7a786ad5d7e.exe
["C:\windows\temp\5a9758fb7e97e044db5cf7a786ad5d7e.exe" ]
Reads from process: PID:1156 C:\Windows\explorer.exe
Terminates process: C:\Windows\Temp\5a9758fb7e97e044db5cf7a786ad5d7e.exe

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex: \Sessions\1\BaseNamedObjects\5a9758fb7e97e044db5cf7a786ad5d7e

## File System Events

Creates:
C:\Users\Admin\AppData\Local\Temp\install_5a9758fb7e97e044db5cf7a786ad5d7e_2016_04_28_15_07.log
Opens: C:\Windows\Prefetch\5A9758FB7E97E044DB5CF7A786AD5-990B9B2F.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\SysWOW64
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\Temp\5a9758fb7e97e044db5cf7a786ad5d7e.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
Opens:
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.9200.16384_none_ba245425e0986353
Opens:
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.9200.16384_none_ba245425e0986353\GdiPlus.dll
Opens: C:\Windows\SysWOW64\fltLib.dll
Opens: C:\Windows\SysWOW64\combase.dll
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\msvcrt.dll
Opens: C:\Windows\SysWOW64\bcryptprimitives.dll
Opens: C:\Windows\SysWOW64\cryptbase.dll
Opens: C:\Windows\SysWOW64\sspicli.dll
Opens: C:\Windows\SysWOW64\rpcrt4.dll
Opens: C:\Windows\SysWOW64\gdi32.dll
Opens: C:\Windows\SysWOW64\user32.dll
Opens: C:\Windows\SysWOW64\psapi.dll
Opens: C:\Windows\SysWOW64\cfgmgr32.dll
Opens: C:\Windows\SysWOW64\devobj.dll

Opens: C:\Windows\SysWOW64\setupapi.dll
Opens: C:\Windows\SysWOW64\advapi32.dll
Opens: C:\Windows\SysWOW64\shlwapi.dll
Opens: C:\Windows\SysWOW64\shell32.dll
Opens: C:\Windows\SysWOW64\ole32.dll
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\SysWOW64\msctf.dll
Opens: C:\Windows\SysWOW64\oleaut32.dll
Opens: C:\Windows\SysWOW64\msasn1.dll
Opens: C:\Windows\SysWOW64\crypt32.dll
Opens: C:\Windows\SysWOW64\wintrust.dll
Opens: C:\Windows\SysWOW64\cryptsp.dll
Opens: C:\Windows\SysWOW64\rsaenh.dll
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\windows\temp\background.png
Writes to: C:\Users\Admin\AppData\Local\Temp\install_5a9758fb7e97e044db5cf7a786ad5d7e_2016_04_28_15_07.log

# Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\wintrust\trust providers\software publishing
Opens key: HKLM\software\microsoft\wow64
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\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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\system\currentcontrolset\control\session manager
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\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\windows\windows error reporting\wmr
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup
Opens key: HKLM\software\microsoft\windows\currentversion\setup
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\system\currentcontrolset\services\crypt32
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\msasn1
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\certificate\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\finalpolicy\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\initialization\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\message\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\signature\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\certcheck\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\diagnosticpolicy\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\cleanup\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft enhanced rsa and aes cryptographic provider
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\deshashsessionkeybackward
Opens key: HKU\
Opens key: HKCU\software\microsoft\internet explorer\security
Opens key:
HKLM\software\wow6432node\policies\microsoft\systemcertificates\trustedpublisher\safer
Opens key:
HKLM\software\policies\microsoft\systemcertificates\trustedpublisher\safer
Opens key:
HKCU\software\policies\microsoft\systemcertificates\trustedpublisher\safer
Opens key:
HKLM\software\wow6432node\microsoft\systemcertificates\trustedpublisher\safer
Opens key: HKLM\software\microsoft\systemcertificates\trustedpublisher\safer
Opens key: HKLM\hardware\devicemap\video
Opens key: HKLM\system\currentcontrolset\control\video\{bf735b18-1b5a-4e14-b64c-f2223c917d28}\0000
Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&1&10
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: 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: HKCU\software\microsoft\windows\currentversion\directmanipulation
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: 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]
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[5a9758fb7e97e044db5cf7a786ad5d7e.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[5a9758fb7e97e044db5cf7a786ad5d7e]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
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\services\crypt32[debugheapflags]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\certificate\{00aac56b-cd44-11d0-
8cc2-00c04fc295ee}[$dll]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\certificate\{00aac56b-cd44-11d0-
8cc2-00c04fc295ee}[$function]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\finalpolicy\{00aac56b-cd44-11d0-
8cc2-00c04fc295ee}[$dll]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\finalpolicy\{00aac56b-cd44-11d0-
8cc2-00c04fc295ee}[$function]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\initialization\{00aac56b-cd44-
11d0-8cc2-00c04fc295ee}[$dll]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\initialization\{00aac56b-cd44-
11d0-8cc2-00c04fc295ee}[$function]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\message\{00aac56b-cd44-11d0-
8cc2-00c04fc295ee}[$dll]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\message\{00aac56b-cd44-11d0-
8cc2-00c04fc295ee}[$function]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\signature\{00aac56b-cd44-11d0-
8cc2-00c04fc295ee}[$dll]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\signature\{00aac56b-cd44-11d0-
8cc2-00c04fc295ee}[$function]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\certcheck\{00aac56b-cd44-11d0-
8cc2-00c04fc295ee}[$dll]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\certcheck\{00aac56b-cd44-11d0-
8cc2-00c04fc295ee}[$function]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\cleanup\{00aac56b-cd44-11d0-
8cc2-00c04fc295ee}[$dll]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\providers\trust\cleanup\{00aac56b-cd44-11d0-

8cc2-00c04fc295ee}[$function]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft enhanced rsa and aes cryptographic provider[type]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft enhanced rsa and aes cryptographic provider[image path]
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: HKCU\software\microsoft\windows\currentversion\wintrust\trust providers\software publishing[state]
Queries value: HKCU\software\microsoft\internet explorer\security[safety warning level]
Queries value: HKLM\system\currentcontrolset\services\crypt32[diaglevel]
Queries value: HKLM\system\currentcontrolset\services\crypt32[diagmatchanymask]
Queries value: HKLM\hardware\devicemap\video[maxobjectnumber]
Queries value: HKLM\hardware\devicemap\video[\device\video0]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000[pruningmode]
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\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\rpc[idletimerwindow]