

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 175, Task ID: 700

Task ID:	700
Risk Level:	8
Date Processed:	2016-04-28 13:06:31 (UTC)
Processing Time:	5.91 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:	00233b752391954234515941d9b1a2fd32753d9c8e03203e107c7c0e09141752
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:1168 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
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX

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\System32
Opens:	C:\windows\temp\5a9758fb7e97e044db5cf7a786ad5d7e.exe.Local\
Opens:	
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80	
Opens:	
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll	
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\FLTLib.DLL
Opens:	C:\Windows\System32\fltLib.dll
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\System32\en-US\setupapi.dll.mui
Opens:	C:\windows\temp\CRYPTSP.dll
Opens:	C:\Windows\System32\cryptsp.dll
Opens:	C:\Windows\System32\rsaenh.dll
Opens:	C:\windows\temp\CRYPTBASE.dll
Opens:	C:\Windows\System32\cryptbase.dll
Opens:	C:\Windows\explorer.exe
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows\System32\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\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\ddl
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
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\ole
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\system\currentcontrolset\control\cmf\config
Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr
Opens key: HKLM\software\microsoft\windows\currentversion\setup
Opens key: HKLM\software\microsoft\windows\currentversion
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\system\currentcontrolset\services\crypt32
Opens key: HKLM\software\microsoft\windows nt\currentversion\msasn1
Opens key: HKLM\software\microsoft\cryptography\providers\trust\certificate\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}
Opens key: HKLM\software\microsoft\cryptography\providers\trust\finalpolicy\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}
Opens key: HKLM\software\microsoft\cryptography\providers\trust\initialization\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}
Opens key: HKLM\software\microsoft\cryptography\providers\trust\message\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}
Opens key: HKLM\software\microsoft\cryptography\providers\trust\signature\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}
Opens key: HKLM\software\microsoft\cryptography\providers\trust\certcheck\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}
Opens key: HKLM\software\microsoft\cryptography\providers\trust\diagnosticpolicy\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}
Opens key: HKLM\software\microsoft\cryptography\providers\trust\cleanup\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft
enhanced rsa and aes cryptographic provider
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\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography\offload
Opens key: HKLM\software\microsoft\cryptography\deshashsessionkeybackward
Opens key: HKU\
Opens key: HKCU\software\microsoft\internet explorer\security
Opens key:

```

HKLM\software\policies\microsoft\systemcertificates\trustedpublisher\safer
  Opens key:
HKCU\software\policies\microsoft\systemcertificates\trustedpublisher\safer
  Opens key: HKLM\software\microsoft\systemcertificates\trustedpublisher\safer
  Opens key: HKLM\software\microsoft\cryptography\wintrust\config
  Opens key: HKLM\software\microsoft\cryptography\oid
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllputsigneddatamsg
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllputsigneddatamsg\{000c10f1-0000-0000-c000-000000000046}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllputsigneddatamsg\{06c9e010-38ce-11d4-a2a3-00104bd35090}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllputsigneddatamsg\{1629f04e-2799-4db5-8fe5-ace10f17ebab}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllputsigneddatamsg\{1a610570-38ce-11d4-a2a3-00104bd35090}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllputsigneddatamsg\{603bcc1f-4b59-4e08-b724-d2c6297ef351}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllputsigneddatamsg\{9ba61d3f-e73a-11d0-8cd2-00c04fc295ee}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllputsigneddatamsg\{ab13f5b1-f718-11d0-82aa-00aa00c065e1}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllputsigneddatamsg\{c689aab8-8e78-11d0-8c47-00c04fc295ee}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllputsigneddatamsg\{c689aab9-8e78-11d0-8c47-00c04fc295ee}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllputsigneddatamsg\{c689aaba-8e78-11d0-8c47-00c04fc295ee}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllputsigneddatamsg\{de351a42-8e59-11d0-8c47-00c04fc295ee}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllputsigneddatamsg\{de351a43-8e59-11d0-8c47-00c04fc295ee}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptsipdllputsigneddatamsg
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgets signeddatamsg
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgets signeddatamsg\{000c10f1-0000-0000-c000-000000000046}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgets signeddatamsg\{06c9e010-38ce-11d4-a2a3-00104bd35090}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgets signeddatamsg\{1629f04e-2799-4db5-8fe5-ace10f17ebab}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgets signeddatamsg\{1a610570-38ce-11d4-a2a3-00104bd35090}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgets signeddatamsg\{603bcc1f-4b59-4e08-b724-d2c6297ef351}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgets signeddatamsg\{9ba61d3f-e73a-11d0-8cd2-00c04fc295ee}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgets signeddatamsg\{ab13f5b1-f718-11d0-82aa-00aa00c065e1}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgets signeddatamsg\{c689aab8-8e78-11d0-8c47-00c04fc295ee}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgets signeddatamsg\{c689aab9-8e78-11d0-8c47-00c04fc295ee}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgets signeddatamsg\{c689aaba-8e78-11d0-8c47-00c04fc295ee}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgets signeddatamsg\{de351a42-8e59-11d0-8c47-00c04fc295ee}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgets signeddatamsg\{de351a43-8e59-11d0-8c47-00c04fc295ee}
  Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptsipdllgets signeddatamsg
  Opens key: HKLM\hardware\devicemap\video
  Opens key: HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000
  Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&0&10
  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\sqlclient\windows
 Opens key: HKLM\software\microsoft\sqlclient\windows
 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\control\session manager[safedllsearchmode]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\compatibility32[5a9758fb7e97e044db5cf7a786ad5d7e]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\windows[loadappinit_dlls]
 Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
 Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]
 Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
 Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
 Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
 Queries value: HKLM\software\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\microsoft\cryptography\providers\trust\certificate\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}[\$dll]
 Queries value:
 HKLM\software\microsoft\cryptography\providers\trust\certificate\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}[\$function]
 Queries value:
 HKLM\software\microsoft\cryptography\providers\trust\finalpolicy\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}[\$dll]
 Queries value:
 HKLM\software\microsoft\cryptography\providers\trust\finalpolicy\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}[\$function]
 Queries value:
 HKLM\software\microsoft\cryptography\providers\trust\initialization\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}[\$dll]
 Queries value:
 HKLM\software\microsoft\cryptography\providers\trust\initialization\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}[\$function]
 Queries value: HKLM\software\microsoft\cryptography\providers\trust\message\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}[\$dll]
 Queries value: HKLM\software\microsoft\cryptography\providers\trust\message\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}[\$function]
 Queries value:
 HKLM\software\microsoft\cryptography\providers\trust\signature\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}[\$dll]
 Queries value:
 HKLM\software\microsoft\cryptography\providers\trust\signature\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}[\$function]
 Queries value:
 HKLM\software\microsoft\cryptography\providers\trust\certcheck\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}[\$dll]
 Queries value:
 HKLM\software\microsoft\cryptography\providers\trust\certcheck\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}[\$function]
 Queries value:
 HKLM\software\microsoft\cryptography\providers\trust\cleanup\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}[\$dll]
 Queries value: HKLM\software\microsoft\cryptography\providers\trust\cleanup\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}[\$function]
 Queries value: HKLM\software\microsoft\cryptography\providers\trust\cleanup\{00aac56b-cd44-11d0-8cc2-00c04fc295ee}[\$function]
 Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft
 enhanced rsa and aes cryptographic provider[type]
 Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft
 enhanced rsa and aes 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: 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\video3]
Queries value: HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-fd27e3774e32}\0000[pruningmode]
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\sqlclient\windows[ceipenable]