Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 175, Task ID: 699

Task ID:	699
Risk Level:	8
Date Processed:	2016-04-28 13:06:31 (UTC)
Processing Time:	5.66 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:1960 C:\WINDOWS\explorer.exe
Terminates process:	C:\WINDOWS\Temp\5a9758fb7e97e044db5cf7a786ad5d7e.exe

Named Object Events

Creates mutex:	\BaseNamedObjects\5a9758fb7e97e044db5cf7a786ad5d7e
Creates mutex:	\BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\install_5a9758fb7e97e044db5cf7a786ad5d7e_2016_04_28_15_06.log
Opens:	C:\WINDOWS\Prefetch\5A9758FB7E97E044DB5CF7A786AD5-07B54A2F.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-

```
ww_dfb54e0c\GdiPlus.dll
  Opens:                    C:\WINDOWS\system32\psapi.dll
  Opens:                    C:\WINDOWS\system32\setupapi.dll
  Opens:                    C:\WINDOWS\system32\fltlib.dll
  Opens:                    C:\WINDOWS\system32\imm32.dll
  Opens:                    C:\WINDOWS\system32\shell32.dll
  Opens:                    C:\WINDOWS\system32\SHELL32.dll.124.Manifest
  Opens:                    C:\WINDOWS\system32\SHELL32.dll.124.Config
  Opens:                    C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
  Opens:                    C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
  Opens:                    C:\WINDOWS\WindowsShell.Manifest
  Opens:                    C:\WINDOWS\WindowsShell.Config
  Opens:                    C:\Documents and Settings\Admin\Local Settings\Temp
  Opens:                    C:\WINDOWS\system32\wintrust.dll
  Opens:                    C:\WINDOWS\system32\crypt32.dll
  Opens:                    C:\WINDOWS\system32\msasn1.dll
  Opens:                    C:\WINDOWS\system32\rsaenh.dll
  Opens:                    C:\WINDOWS\explorer.exe
  Opens:                    C:\WINDOWS\system32\MSCTF.dll
  Opens:                    C:\WINDOWS\system32\MSCTFIME.IME
  Opens:                    C:\windows\temp\background.png
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\install_5a9758fb7e97e044db5cf7a786ad5d7e_2016_04_28_15_06.log
  Reads from:               C:\WINDOWS\system32\rsaenh.dll
```

Windows Registry Events

```
  Creates key:              HKCU\software\microsoft\windows\currentversion\wintrust\trust
providers\software publishing
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\5a9758fb7e97e044db5cf7a786ad5d7e.exe
  Opens key:                HKLM\system\currentcontrolset\control\terminal server
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:                HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\winlogon
  Opens key:                HKLM\
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll
  Opens key:                HKLM\system\currentcontrolset\control\session manager
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\gdiplus.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\psapi.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\setupapi.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\fltlib.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
  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:              HKCR\interface
  Opens key:              HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:              HKCU\
  Opens key:              HKCU\software\policies\microsoft\control panel\desktop
  Opens key:              HKCU\control panel\desktop
  Opens key:              HKLM\system\setup
  Opens key:              HKLM\system\currentcontrolset\control\minint
  Opens key:              HKLM\system\wpa\pnp
  Opens key:              HKLM\software\microsoft\windows\currentversion\setup
  Opens key:              HKLM\software\microsoft\windows\currentversion
  Opens key:              HKLM\software\microsoft\windows\currentversion\setup\apploglevels
  Opens key:              HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:              HKLM\system\currentcontrolset\services\tcpip\parameters
  Opens key:              HKLM\software\policies\microsoft\system\dnsclient
  Opens key:              HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll
  Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\languagepack
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msasn1.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\crypt32.dll
  Opens key:              HKLM\system\currentcontrolset\services\crypt32\performance
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\msasn1
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imagehlp.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wintrust.dll
  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:             HKCU\software\microsoft\cryptography\providers\type 001
  Opens key:             HKLM\software\microsoft\cryptography\defaults\provider types\type 001
  Opens key:             HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
  Opens key:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
  Opens key:             HKLM\software\policies\microsoft\cryptography
  Opens key:             HKLM\software\microsoft\cryptography
  Opens key:             HKLM\software\microsoft\cryptography\offload
  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\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\{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\cryptsipdllgetsigneddatamsg
  Opens key:             HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgetsigneddatamsg\{000c10f1-0000-0000-c000-000000000046}
  Opens key:             HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgetsigneddatamsg\{06c9e010-38ce-11d4-a2a3-00104bd35090}
  Opens key:             HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgetsigneddatamsg\{1629f04e-2799-4db5-8fe5-ace10f17ebab}
  Opens key:             HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgetsigneddatamsg\{1a610570-38ce-11d4-a2a3-00104bd35090}
  Opens key:             HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgetsigneddatamsg\{9ba61d3f-e73a-11d0-8cd2-00c04fc295ee}
```

```
  Opens key:                 HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgetsigneddatamsg\{ab13f5b1-f718-11d0-82aa-00aa00c065e1}
  Opens key:                 HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgetsigneddatamsg\{c689aab8-8e78-11d0-8c47-00c04fc295ee}
  Opens key:                 HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgetsigneddatamsg\{c689aab9-8e78-11d0-8c47-00c04fc295ee}
  Opens key:                 HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgetsigneddatamsg\{c689aaba-8e78-11d0-8c47-00c04fc295ee}
  Opens key:                 HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgetsigneddatamsg\{de351a42-8e59-11d0-8c47-00c04fc295ee}
  Opens key:                 HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptsipdllgetsigneddatamsg\{de351a43-8e59-11d0-8c47-00c04fc295ee}
  Opens key:                 HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptsipdllgetsigneddatamsg
  Opens key:                 HKLM\hardware\devicemap\video
  Opens key:                 HKLM\software\microsoft\rpc\pagedbuffers
  Opens key:                 HKLM\software\microsoft\rpc
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\5a9758fb7e97e044db5cf7a786ad5d7e.exe\rpcthreadpoolthrottle
  Opens key:                 HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\5a9758fb7e97e044db5cf7a786ad5d7e.exe
  Opens key:                 HKLM\software\microsoft\ctf\systemshared\
  Opens key:                 HKCU\keyboard layout\toggle
  Opens key:                 HKLM\software\microsoft\ctf\
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\imm
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
  Opens key:                 HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctfime.ime
  Opens key:                 HKCU\software\microsoft\ctf
  Opens key:                 HKLM\software\microsoft\ctf\systemshared
  Queries value:             HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:             HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  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\ime
compatibility[5a9758fb7e97e044db5cf7a786ad5d7e]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:             HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
  Queries value:             HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Queries value:             HKCR\interface[interfacehelperdisableall]
  Queries value:             HKCR\interface[interfacehelperdisableallforole32]
  Queries value:             HKCR\interface[interfacehelperdisabletypelib]
  Queries value:             HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
  Queries value:             HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
  Queries value:             HKCU\control panel\desktop[multiuilanguageid]
  Queries value:             HKLM\system\setup[systemsetupinprogress]
  Queries value:             HKLM\system\wpa\pnp[seed]
  Queries value:             HKLM\system\setup[osloaderpath]
  Queries value:             HKLM\system\setup[systempartition]
  Queries value:            HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
  Queries value:            HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
  Queries value:            HKLM\software\microsoft\windows\currentversion[devicepath]
  Queries value:            HKLM\software\microsoft\windows\currentversion\setup[loglevel]
  Queries value:            HKLM\software\microsoft\windows\currentversion\setup[logpath]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
  Queries value:            HKCU\control panel\desktop[smoothscroll]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  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\defaults\provider types\type
001[name]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  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\hardware\devicemap\video[maxobjectnumber]
  Queries value:              HKLM\hardware\devicemap\video[\device\video0]
  Queries value:              HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:              HKLM\software\microsoft\ctf\systemshared[cuas]
  Queries value:              HKCU\keyboard layout\toggle[language hotkey]
  Queries value:              HKCU\keyboard layout\toggle[hotkey]
  Queries value:              HKCU\keyboard layout\toggle[layout hotkey]
  Queries value:              HKLM\software\microsoft\ctf[enableanchorcontext]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
  Queries value:              HKCU\software\microsoft\ctf[disable thread input manager]
  Value changes:              HKLM\software\microsoft\cryptography\rng[seed]
```