

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 131, Task ID: 523

Task ID:	523
Risk Level:	4
Date Processed:	2016-04-28 13:01:23 (UTC)
Processing Time:	3.05 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\2a3d6128a1b210860531603f74a24c7f.exe"
Sample ID:	131
Type:	basic
Owner:	admin
Label:	2a3d6128a1b210860531603f74a24c7f
Date Added:	2016-04-28 12:45:03 (UTC)
File Type:	PE32:win32:gui
File Size:	620911 bytes
MD5:	2a3d6128a1b210860531603f74a24c7f
SHA256:	cca1510e63a3ab7c4679ab5043dd4c3e0ba1dfcab2e36c67edd3d46793a8134
Description:	None

Pattern Matching Results

- 2 PE: Nonstandard section
- 4 Packer: NSIS [Nullsoft Scriptable Install System]

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\2a3d6128a1b210860531603f74a24c7f.exe
["c:\windows\temp\2a3d6128a1b210860531603f74a24c7f.exe"]	
Terminates process:	C:\WINDOWS\Temp\2a3d6128a1b210860531603f74a24c7f.exe

Named Object Events

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-1-5-21-1757981266-507921405-1957994488-1003
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore:	\BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}

File System Events

Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsg1.tmp
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsk2.tmp
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsu3.tmp
Creates:	C:\DOCUME~1
Creates:	C:\DOCUME~1\Admin
Creates:	C:\DOCUME~1\Admin\LOCALS~1
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsu3.tmp\nsHelper.dll
Opens:	C:\WINDOWS\Prefetch\2A3D6128A1B210860531603F74A24-3B588113.pf
Opens:	C:\Documents and Settings\Admin
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\Temp\2a3d6128a1b210860531603f74a24c7f.exe

```

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\WindowsShell.Manifest
Opens: C:\WINDOWS\WindowsShell.Config
Opens: C:\WINDOWS\system32\rpcss.dll
Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\WINDOWS\system32\shfolder.dll
Opens: C:\WINDOWS\system32\setupapi.dll
Opens: C:\
Opens: C:\Documents and Settings
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsg1.tmp
Opens: C:\WINDOWS\Temp\e6c9f223-90df-4c80-ad0f-573a446f9a6e
Opens: C:\Documents and Settings\Admin\Local Settings\Temp
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\nsu3.tmp
Opens: C:\Documents and Settings\Admin\Local
Settings\Temp\nsu3.tmp\nsHelper.dll
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\nsu3.tmp\nsHelper.dll.2.Manifest
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\nsu3.tmp\nsHelper.dll.2.Config
Opens: C:\WINDOWS\system32\urlmon.dll.123.Manifest
Opens: C:\WINDOWS\system32\urlmon.dll.123.Config
Opens: C:\Program Files\XingHaoLyrics\
Opens: C:\Program Files\LyricsPal\
Opens: C:\Documents and Settings\Admin\Local Settings
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\nsk2.tmp
Writes to: C:\Documents and Settings\Admin\Local
Settings\Temp\nsu3.tmp\nsHelper.dll
Reads from: C:\WINDOWS\Temp\2a3d6128a1b210860531603f74a24c7f.exe
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\nsk2.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsg1.tmp
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\nsu3.tmp
Deletes: C:\Documents and Settings\Admin\Local
Settings\Temp\nsu3.tmp\nsHelper.dll

```

Windows Registry Events

```

Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\2a3d6128a1b210860531603f74a24c7f.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\gdi32.dll
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\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\image file execution
options\msvcrt.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\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.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\version.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\windows nt\currentversion\winlogon
 Opens key: HKLM\
 Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
 Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance
 Opens key: HKLM\system\setup
 Opens key: HKCU\
 Opens key: HKCU\software\policies\microsoft\control panel\desktop
 Opens key: HKCU\control panel\desktop
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
 Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
 Opens key: HKLM\software\microsoft\ole
 Opens key: HKCR\interface
 Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msctf.dll
 Opens key: HKLM\software\microsoft\ctf\compatibility\2a3d6128a1b210860531603f74a24c7f.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\image file execution

options\shfolder.dll
 Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
 Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\2a3d6128a1b210860531603f74a24c7f.exe
 Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-a2d8-08002b30309d}
 Opens key: HKCU\software\classes\
 Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32
 Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\setupapi.dll
 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\rpc\pagedbuffers
 Opens key: HKLM\software\microsoft\rpc
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\2a3d6128a1b210860531603f74a24c7f.exe\rpcthreadpoolthrottle
 Opens key: HKLM\software\policies\microsoft\windows nt\rpc
 Opens key: HKLM\system\currentcontrolset\control\computername
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-11e3-9fc7-806d6172696f}
 Opens key: HKCU\software\classes\drive\shellex\folderextensions
 Opens key: HKCR\drive\shellex\folderextensions
 Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
 Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
 Opens key: HKCU\software\classes\directory
 Opens key: HKCR\directory
 Opens key: HKCU\software\classes\directory\curver
 Opens key: HKCR\directory\curver
 Opens key: HKCR\directory\

Opens key: HKCU\software\microsoft\windows\currentversion\explorer
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\system
 Opens key: HKCU\software\classes\directory\shellex\iconhandler
 Opens key: HKCR\directory\shellex\iconhandler
 Opens key: HKCU\software\classes\directory\clsid
 Opens key: HKCR\directory\clsid
 Opens key: HKCU\software\classes\folder
 Opens key: HKCR\folder
 Opens key: HKCU\software\classes\folder\clsid
 Opens key: HKCR\folder\clsid
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\oleaut32.dll
 Opens key: HKLM\software\microsoft\oleaut
 Opens key: HKLM\software\microsoft\oleaut\userera
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\iertutil.dll
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\urlmon.dll
 Opens key: HKCU\software\classes\protocols\name-space handler\
 Opens key: HKCR\protocols\name-space handler
 Opens key: HKCU\software\classes\protocols\name-space handler
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
 settings
 Opens key: HKLM\software\microsoft\windows\currentversion\internet settings
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
 settings
 Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_protocol_lockdown
 Opens key: HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_protocol_lockdown
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
 settings\
 Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
 Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol
 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol
 Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
 Opens key: HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
 settings\zonemap\domains\
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
 settings\zonemap\domains\
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
 settings\zonemap\ranges\
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
 settings\zonemap\ranges\
 Opens key: HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_unc_savedfilecheck
 Opens key: HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_unc_savedfilecheck
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\shhelper.dll
 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\session manager[safedllsearchmode]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\compatibility32[2a3d6128a1b210860531603f74a24c7f]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
 compatibility[2a3d6128a1b210860531603f74a24c7f]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
 Queries value: HKLM\system\setup[systemsetupinprogress]
 Queries value: HKCU\control panel\desktop[multiuianguageid]
 Queries value: HKCU\control panel\desktop[smoothscroll]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
 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: 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:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
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: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-11e3-9fc7-806d6172696f}[data]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-11e3-9fc7-806d6172696f}[generation]
Queries value: HKCR\drive\shellex\folderextensions\{fbcb8a05-beee-4442-804e-409d6c4515e9}[drivemask]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
Queries value: HKCR\directory[docobject]
Queries value: HKCR\directory[browseinplace]
Queries value: HKCR\directory[isshortcut]
Queries value: HKCR\directory[alwaysshowext]
Queries value: HKCR\directory[nevershowext]
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[2a3d6128a1b210860531603f74a24c7f.exe]
Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]
Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}[baseclass]