Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 59, Task ID: 235

Task ID:	235
Risk Level:	4
Date Processed:	2016-04-28 12:53:42 (UTC)
Processing Time:	61.09 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\394c529a998f001b2544559ea85b0e07.exe"
Sample ID:	59
Type:	basic
Owner:	admin
Label:	394c529a998f001b2544559ea85b0e07
Date Added:	2016-04-28 12:44:55 (UTC)
File Type:	PE32:win32:gui
File Size:	757856 bytes
MD5:	394c529a998f001b2544559ea85b0e07
SHA256:	fdf973b3a46c7aa7bbf3f4235cbf3b2d77247c11eedf287861d334ba4275e5ce
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\394c529a998f001b2544559ea85b0e07.exe ["c:\windows\temp\394c529a998f001b2544559ea85b0e07.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-1-5-21-1757981266-507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates event:	\BaseNamedObjects\userenv: User Profile setup event
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore:	\BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}
Creates semaphore:	\BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

File System Events

Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsp1.tmp
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsw2.tmp
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.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:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\System.dll
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\lua51.dll
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\LuaXml_lib.dll
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\LuaBridge.dll
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\definitions.lua
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\utils.lua
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\LuaBridge.dll
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\LuaSocket
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\LuaSocket\socket
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\LuaSocket
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\LuaSocket\mime

```
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\mime.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\ltn12.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\http.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\ftp.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\tp.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\smtp.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\url.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\socket\core.dll
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\mime\core.dll
  Creates:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\LuaXml.lua
  Creates:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\json.lua
  Creates:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\luacom.dll
  Creates:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\Env.lua
  Creates:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\Sandbox.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\BundleInstall.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\Downloads.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\NotifyIcon.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\CallbackProxy.lua
  Creates:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\UiState.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\ProcessFreeFile.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\extension.tlb
  Creates:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\GuiInit.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\DownloadList.lua
  Creates:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\Events.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\DownloadThread.lua
  Creates:               C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\System.dll
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\IntegratedOffer.lua
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\BrowserControl.lua
  Creates:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\res
  Creates:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\bullet
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\res\jquery.js
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\res\common.js
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\res\common.css
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\res\knockout.js
  Creates:               C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\bullet
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\accept.png
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\back.png
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\cancel.png
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\close.png
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\decline.png
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\next.png
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\progress.gif
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\progressPause.gif
  Creates:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\skin.jpg
  Creates:               C:\Documents and Settings\Admin\Local
```

```
Settings\Temp\nsw3.tmp\__localxml.xml
  Creates:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\AdvancedTests.lua
  Creates:                C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\version.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\UACInfo.dll
  Creates:                C:\Documents and Settings\Admin\My Documents\My Videos
  Creates:                C:\Documents and Settings\Admin\My Documents\My Videos\Desktop.ini
  Creates:                C:\Documents and Settings\Admin\Start Menu\Programs\Administrative Tools
  Creates:                C:\Documents and Settings\Admin\Start Menu\Programs\Administrative
Tools\desktop.ini
  Creates:                C:\WINDOWS\Resources\0409
  Creates:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\FloatingProgress.dll
  Creates:                C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\FloatingProgress.dll
  Creates:                C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\__web.xml
  Opens:                  C:\WINDOWS\Prefetch\394C529A998F001B2544559EA85B0-109AC412.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\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\nsp1.tmp
  Opens:                  C:\WINDOWS\Temp\7790ae57-8163-4eeb-aee6-c248c9ab2dda
  Opens:                  C:\WINDOWS\Temp\394c529a998f001b2544559ea85b0e07.exe
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\System.dll
  Opens:                  C:\WINDOWS\system32\winmm.dll
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaBridge.dll
  Opens:                  C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\LuaBridge.dll.2.Manifest
  Opens:                  C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\LuaBridge.dll.2.Config
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\lua51.dll
  Opens:                  C:\WINDOWS\system32\iphlpapi.dll
  Opens:                  C:\WINDOWS\system32\ws2_32.dll
  Opens:                  C:\WINDOWS\system32\ws2help.dll
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\definitions.lua
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\utils.lua
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\socket
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\mime
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\GuiInit.lua
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\473cc25d62ab653c6f7e53a704dc6e0ff7a8b71b
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\473cc25d62ab653c6f7e53a704dc6e0ff7a8b71b.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\LuaXml.lua
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\d5d7f3f32daa4938801b818601d43b728214a756
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\d5d7f3f32daa4938801b818601d43b728214a756.dll
  Opens:                  C:LuaXML_lib.lua
  Opens:                  C:\windows\temp\lua\LuaXML_lib.lua
  Opens:                  C:\windows\temp\lua\LuaXML_lib\init.lua
  Opens:                  C:\windows\temp\LuaXML_lib.lua
  Opens:                  C:\windows\temp\LuaXML_lib\init.lua
  Opens:                  C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\LuaXML_lib.lua
  Opens:                  C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\LuaSocket\lua\LuaXML_lib.lua
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaXml_lib.dll
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\897d21056a341314b60764c31b36c1fad542e78a
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\897d21056a341314b60764c31b36c1fad542e78a.dll
  Opens:                  C:socket.lua
  Opens:                 C:\windows\temp\lua\socket.lua
  Opens:                 C:\windows\temp\lua\socket\init.lua
  Opens:                 C:\windows\temp\socket.lua
  Opens:                 C:\windows\temp\socket\init.lua
  Opens:                 C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\socket.lua
  Opens:                 C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket.lua
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\87a5250e7389d052be3fdc257872ebd873ef2deb
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\87a5250e7389d052be3fdc257872ebd873ef2deb.dll
  Opens:                 C:socket\core.lua
  Opens:                 C:\windows\temp\lua\socket\core.lua
  Opens:                 C:\windows\temp\lua\socket\core\init.lua
  Opens:                 C:\windows\temp\socket\core.lua
  Opens:                 C:\windows\temp\socket\core\init.lua
  Opens:                 C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\socket\core.lua
  Opens:                 C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\LuaSocket\lua\socket\core.lua
  Opens:                 C:socket\core.dll
  Opens:                 C:\windows\temp\socket\core.dll
  Opens:                 C:\windows\temp\loadall.dll
  Opens:                 C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\socket\core.dll
  Opens:                 C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\socket\core.dll
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\7b33b2bde409277581a53da83ac5b1bfdcf29afa
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\7b33b2bde409277581a53da83ac5b1bfdcf29afa.dll
  Opens:                 C:socket\http.lua
  Opens:                 C:\windows\temp\lua\socket\http.lua
  Opens:                 C:\windows\temp\lua\socket\http\init.lua
  Opens:                 C:\windows\temp\socket\http.lua
  Opens:                 C:\windows\temp\socket\http\init.lua
  Opens:                 C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\socket\http.lua
  Opens:                 C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\http.lua
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\c27913efc6edcc938c504fa24651c7f3d95f51cc
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\c27913efc6edcc938c504fa24651c7f3d95f51cc.dll
  Opens:                 C:socket\url.lua
  Opens:                 C:\windows\temp\lua\socket\url.lua
  Opens:                 C:\windows\temp\lua\socket\url\init.lua
  Opens:                 C:\windows\temp\socket\url.lua
  Opens:                 C:\windows\temp\socket\url\init.lua
  Opens:                 C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\socket\url.lua
  Opens:                 C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\url.lua
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\7d4b85d62fb353e7a43256f40d539ceb6fd06006
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\7d4b85d62fb353e7a43256f40d539ceb6fd06006.dll
  Opens:                 C:ltn12.lua
  Opens:                 C:\windows\temp\lua\ltn12.lua
  Opens:                 C:\windows\temp\lua\ltn12\init.lua
  Opens:                 C:\windows\temp\ltn12.lua
  Opens:                 C:\windows\temp\ltn12\init.lua
  Opens:                 C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\ltn12.lua
  Opens:                 C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\ltn12.lua
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\c6d51ab09f96b7569326130e860517b7d87e866d
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\c6d51ab09f96b7569326130e860517b7d87e866d.dll
  Opens:                 C:mime.lua
  Opens:                 C:\windows\temp\lua\mime.lua
  Opens:                 C:\windows\temp\lua\mime\init.lua
  Opens:                 C:\windows\temp\mime.lua
  Opens:                 C:\windows\temp\mime\init.lua
  Opens:                 C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\mime.lua
  Opens:                 C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\mime.lua
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\f40368059830399ce8189100003d317f2739d087
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\f40368059830399ce8189100003d317f2739d087.dll
  Opens:                 C:mime\core.lua
  Opens:                 C:\windows\temp\lua\mime\core.lua
  Opens:                 C:\windows\temp\lua\mime\core\init.lua
  Opens:                 C:\windows\temp\mime\core.lua
  Opens:                 C:\windows\temp\mime\core\init.lua
  Opens:                 C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\mime\core.lua
  Opens:                 C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\LuaSocket\lua\mime\core.lua
  Opens:                  C:mime\core.dll
  Opens:                  C:\windows\temp\mime\core.dll
  Opens:                  C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\mime\core.dll
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\mime\core.dll
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\f45008e3c900e7920effac3ed6f377dd0caf0cf1
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\f45008e3c900e7920effac3ed6f377dd0caf0cf1.dll
  Opens:                  C:socket\ftp.lua
  Opens:                  C:\windows\temp\lua\socket\ftp.lua
  Opens:                  C:\windows\temp\lua\socket\ftp\init.lua
  Opens:                  C:\windows\temp\socket\ftp.lua
  Opens:                  C:\windows\temp\socket\ftp\init.lua
  Opens:                  C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\socket\ftp.lua
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\ftp.lua
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\a317db596f44efe64d2468fcc06f25e9e5c24881
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\a317db596f44efe64d2468fcc06f25e9e5c24881.dll
  Opens:                  C:socket\tp.lua
  Opens:                  C:\windows\temp\lua\socket\tp.lua
  Opens:                  C:\windows\temp\lua\socket\tp\init.lua
  Opens:                  C:\windows\temp\socket\tp.lua
  Opens:                  C:\windows\temp\socket\tp\init.lua
  Opens:                  C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\socket\tp.lua
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\tp.lua
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\05d97e6e9834ccf063c552e404b9ecafc5e4d662
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\05d97e6e9834ccf063c552e404b9ecafc5e4d662.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\json.lua
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\9ed037b84943c4caa3a520e48a5540181c46c98c
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\9ed037b84943c4caa3a520e48a5540181c46c98c.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\Sandbox.lua
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\a2562690818adae41c773c584b6f6c09ebb4d39c
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\a2562690818adae41c773c584b6f6c09ebb4d39c.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\Env.lua
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\54785412a7c2f25a4535a5b8a463d4b9c179408b
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\54785412a7c2f25a4535a5b8a463d4b9c179408b.dll
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\CallbackProxy.lua
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\a862c2b21b5e1337de2b76d5e43ae1375117d34d
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\a862c2b21b5e1337de2b76d5e43ae1375117d34d.dll
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\Downloads.lua
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\DownloadList.lua
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\Events.lua
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\DownloadThread.lua
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\BrowserControl.lua
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\1feb3ea612cdf9b90056427956a6421e260272ab
  Opens:
C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\1feb3ea612cdf9b90056427956a6421e260272ab.dll
  Opens:                  C:luacom.lua
  Opens:                  C:\windows\temp\lua\luacom.lua
  Opens:                  C:\windows\temp\lua\luacom\init.lua
  Opens:                  C:\windows\temp\luacom.lua
  Opens:                  C:\windows\temp\luacom\init.lua
  Opens:                  C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\luacom.lua
  Opens:                  C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\LuaSocket\lua\luacom.lua
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\luacom.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\res
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\bullet
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\AdvancedTests.lua
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\version.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\UACInfo.dll
  Opens:                  C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\UACInfo.dll.2.Manifest
  Opens:                  C:\DOCUME~1\Admin\LOCALS~1\Temp\nsw3.tmp\UACInfo.dll.2.Config
  Opens:                  C:\Documents and Settings\Admin\My Documents\My Videos\Desktop.ini
  Opens:                  C:\Documents and Settings\Admin\My Documents\My Videos
  Opens:                  C:\WINDOWS\system32\netapi32.dll
  Opens:                  C:\Documents and Settings\Admin\Start Menu\desktop.ini
  Opens:                  C:\Documents and Settings\Admin\Start Menu
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\desktop.ini
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Administrative Tools
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Administrative
Tools\desktop.ini
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\FloatingProgress.dll
  Opens:                  C:\WINDOWS\system32\MSCTFIME.IME
  Opens:                  C:\WINDOWS\system32\uxtheme.dll
  Opens:                  C:\WINDOWS\system32\MSIMTF.dll
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\__localxml.xml
  Opens:                  C:\WINDOWS\system32\mswsock.dll
  Opens:                  C:\WINDOWS\system32\hnetcfg.dll
  Opens:                  C:\WINDOWS\system32\wshtcpip.dll
  Opens:                  C:\WINDOWS\system32\dnsapi.dll
  Opens:                  C:\WINDOWS\system32\winrnr.dll
  Opens:                  C:\WINDOWS\system32\drivers\etc\hosts
  Opens:                  C:\WINDOWS\system32\rsaenh.dll
  Opens:                  C:\WINDOWS\system32\crypt32.dll
  Opens:                  C:\WINDOWS\system32\rasadhlp.dll
  Writes to:              C:\Documents and Settings\Admin\Local Settings\Temp\nsw2.tmp
  Writes to:              C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\System.dll
  Writes to:              C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\lua51.dll
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaXml_lib.dll
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaBridge.dll
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\definitions.lua
  Writes to:              C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\utils.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\mime.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\ltn12.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\http.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\ftp.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\tp.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\smtp.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\url.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\socket\core.dll
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\mime\core.dll
  Writes to:              C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\LuaXml.lua
  Writes to:              C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\json.lua
  Writes to:              C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\luacom.dll
  Writes to:              C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\Env.lua
  Writes to:              C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\Sandbox.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\BundleInstall.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\Downloads.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\NotifyIcon.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\CallbackProxy.lua
  Writes to:              C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\UiState.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\ProcessFreeFile.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\extension.tlb
  Writes to:              C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\GuiInit.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\DownloadList.lua
  Writes to:              C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\Events.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\DownloadThread.lua
  Writes to:              C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\IntegratedOffer.lua
  Writes to:              C:\Documents and Settings\Admin\Local
```

```
Settings\Temp\nsw3.tmp\BrowserControl.lua
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\res\jquery.js
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\res\common.js
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\res\common.css
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\res\knockout.js
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\accept.png
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\back.png
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\cancel.png
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\close.png
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\decline.png
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\next.png
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\progress.gif
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\progressPause.gif
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\bullet\skin.jpg
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\__localxml.xml
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\AdvancedTests.lua
  Writes to:                C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\version.dll
  Writes to:                C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\UACInfo.dll
  Writes to:                C:\Documents and Settings\Admin\My Documents\My Videos\Desktop.ini
  Writes to:                C:\Documents and Settings\Admin\Start Menu\Programs\Administrative
Tools\desktop.ini
  Writes to:                C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\FloatingProgress.dll
  Reads from:               C:\WINDOWS\Temp\394c529a998f001b2544559ea85b0e07.exe
  Reads from:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw2.tmp
  Reads from:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\definitions.lua
  Reads from:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\utils.lua
  Reads from:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\GuiInit.lua
  Reads from:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\LuaXml.lua
  Reads from:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket.lua
  Reads from:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\http.lua
  Reads from:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\url.lua
  Reads from:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\ltn12.lua
  Reads from:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\mime.lua
  Reads from:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\ftp.lua
  Reads from:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\LuaSocket\lua\socket\tp.lua
  Reads from:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\json.lua
  Reads from:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\Sandbox.lua
  Reads from:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\Env.lua
  Reads from:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\CallbackProxy.lua
  Reads from:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\Downloads.lua
  Reads from:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\DownloadList.lua
  Reads from:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp\Events.lua
  Reads from:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\DownloadThread.lua
  Reads from:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\BrowserControl.lua
  Reads from:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\AdvancedTests.lua
  Reads from:               C:\Documents and Settings\Admin\My Documents\My Videos\Desktop.ini
  Reads from:               C:\Documents and Settings\Admin\Start Menu\desktop.ini
  Reads from:               C:\Documents and Settings\Admin\Start Menu\Programs\desktop.ini
  Reads from:               C:\Documents and Settings\Admin\Start Menu\Programs\Administrative
Tools\desktop.ini
  Reads from:               C:\Documents and Settings\Admin\Local
Settings\Temp\nsw3.tmp\__localxml.xml
  Reads from:               C:\WINDOWS\system32\drivers\etc\hosts
  Reads from:            C:\WINDOWS\system32\rsaenh.dll
  Deletes:               C:\Documents and Settings\Admin\Local Settings\Temp\nsp1.tmp
  Deletes:               C:\Documents and Settings\Admin\Local Settings\Temp\nsw3.tmp
```

Network Events

```
  DNS query:             service.downloadadmin.com
  DNS response:          service.downloadadmin.com ⇒ 50.22.63.138
  DNS response:          service.downloadadmin.com ⇒ 50.22.63.140
  Connects to:           50.22.63.138:80
  Connects to:           50.22.63.140:80
  Sends data to:         8.8.8.8:53
  Sends data to:         0.0.0.0:0
  Receives data from:    0.0.0.0:0
  Receives data from:    service.downloadadmin.com:80 (50.22.63.138)
  Receives data from:    service.downloadadmin.com:80 (50.22.63.140)
```

Windows Registry Events

```
  Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-
806d6172696f}\
  Creates key:           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Creates key:           HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Creates key:           HKLM\system\currentcontrolset\services\tcpip\parameters
  Opens key:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\394c529a998f001b2544559ea85b0e07.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\394c529a998f001b2544559ea85b0e07.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\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\394c529a998f001b2544559ea85b0e07.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\system.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winmm.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\drivers32
  Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\lua51.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
  Opens key:                 HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key:                 HKLM\system\currentcontrolset\services\tcpip\parameters\
  Opens key:                 HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
  Opens key:                 HKLM\system\currentcontrolset\services\netbt\parameters
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\luabridge.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\luaxml_lib.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\core.dll
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
  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\luacom.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uacinfo.dll
  Opens key:
HKCU\software\microsoft\windows\shell\associations\urlassociations\http\userchoice
  Opens key:                HKCU\software\classes\http\shell\open\command
  Opens key:                HKLM\software\microsoft\internet explorer
  Opens key:                HKLM\software\mozilla\mozilla firefox
  Opens key:                HKLM\software\microsoft\net framework setup\ndp
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netapi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
  Opens key:                HKLM\system\currentcontrolset\control\productoptions
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:                HKLM\software\policies\microsoft\windows\system
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003
  Opens key:                HKCU\software\microsoft\windows\shellnoroam
  Opens key:                HKU\
  Opens key:                HKCU\software\microsoft\windows\shellnoroam\muicache
  Opens key:                HKCU\software\microsoft\windows\shellnoroam\muicache\
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\floatingprogress.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\imm
  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
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\uxtheme.dll
  Opens key:                HKCU\software\microsoft\windows\currentversion\thememanager
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mswsock.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetcfg.dll
  Opens key:                HKLM\software\microsoft\rpc\securityservice
  Opens key:                HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.dll
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\parameters
  Opens key:                HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wldap32.dll
  Opens key:                HKLM\system\currentcontrolset\services\ldap
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winrnr.dll
  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:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasadhlp.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[394c529a998f001b2544559ea85b0e07]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[394c529a998f001b2544559ea85b0e07]
  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[multiuilanguageid]
  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\{fbeb8a05-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 nt\currentversion\drivers32[wave]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
  Queries value:               HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
```

```
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
   Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
```

```
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[enabledhcp]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseobtainedtime]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseterminatestime]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpserver]
  Queries value:            HKLM\software\microsoft\internet explorer[version]
  Queries value:            HKLM\software\microsoft\windows\currentversion[programfilesdir]
  Queries value:            HKLM\software\microsoft\windows\currentversion[commonfilesdir]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[start menu]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[programs]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[startup]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[sendto]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[recent]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[favorites]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[my music]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[my pictures]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[my video]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer[usesystemforsystemfolders]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[nethood]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[fonts]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[templates]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[printhood]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
```

```
folders[history]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
  Queries value:            HKLM\system\currentcontrolset\control\productoptions[producttype]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local settings]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileimagepath]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[administrative tools]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[flags]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[state]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[userpreference]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[centralprofile]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileloadtimelow]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileloadtimehigh]
  Queries value:            HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
  Queries value:            HKCU\software\microsoft\windows\shellnoroam\muicache[@shell32.dll,-
21762]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cd burning]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
  Queries value:            HKCU\software\microsoft\ctf[disable thread input manager]
  Queries value:            HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
  Queries value:            HKCU\control panel\desktop[lamebuttontext]
  Queries value:            HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
  Queries value:            HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
  Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
  Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
```

```
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
   Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
   Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
   Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[queryadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpdomain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[ipautoconfigurationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[addresstype]
```

```
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpnameserver]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
  Queries value:            HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  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:            HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
  Value changes:            HKLM\software\microsoft\cryptography\rng[seed]
  Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-
806d6172696f}[baseclass]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[desktop]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[start menu]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[programs]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[startup]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[personal]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[sendto]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[recent]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[favorites]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell folders[my
music]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell folders[my
pictures]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell folders[my
video]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[nethood]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[fonts]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[templates]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[local appdata]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[printhood]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cookies]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[history]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[administrative tools]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cd
burning]
```