VALKYRIE COMODO

Summary

File Name: None

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

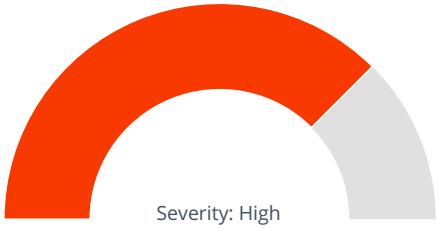
SHA1: 267ef53ea1a203e5181a3ab0d7ad860085834b19

MD5: 4693fd2fba5e6d8a8c15699152edddaf

MALWARE

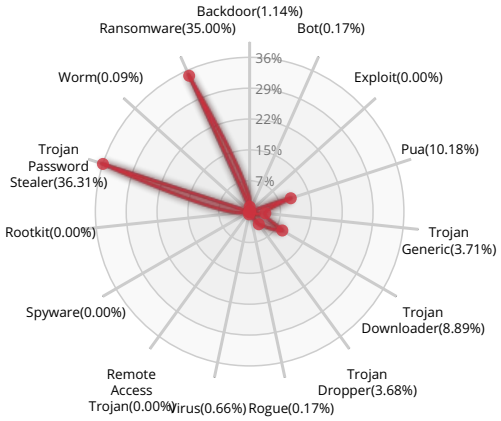
Valkyrie Final Verdict

DETECTION SECTION

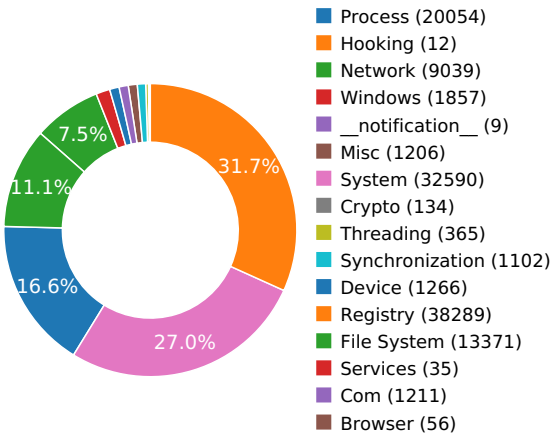


Verdict: Malware

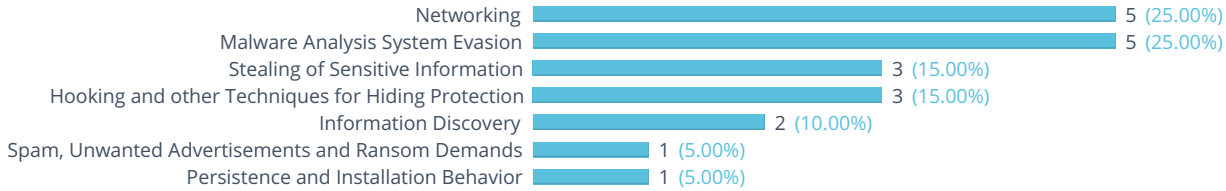
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Expresses interest in specific running processes	Show sources
Reads data out of its own binary image	Show sources

NETWORKING

Attempts to connect to a dead IP:Port (54 unique times)	Show sources
HTTP traffic contains suspicious features which may be indicative of malware related traffic	Show sources
Performs some HTTP requests	Show sources
Network activity contains more than one unique useragent.	Show sources
Generates some ICMP traffic	

STEALING OF SENSITIVE INFORMATION

Attempts to create or modify a Browser Helper Object	Show sources
Steals private information from local Internet browsers	Show sources
Attempts to modify proxy settings	

SPAM, UNWANTED ADVERTISEMENTS AND RANSOM DEMANDS

Exhibits possible ransomware file modification behavior	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources
A named pipe was used for inter-process communication	Show sources
Code injection with CreateRemoteThread in a remote process	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Mimics the system's user agent string for its own requests	Show sources
Possible date expiration check, exits too soon after checking local time	Show sources
A process attempted to delay the analysis task.	Show sources
Creates a hidden or system file	Show sources
Clears web history	Show sources

VALKYRIE COMODO

Behavior Graph

05:14:35 **05:15:54** **05:17:13**

PID 2940

05:14:35 | Create Process | The malicious file created a child process as 267ef53ea1a203e5181a3ab0d7ad860085834b19.exe **(PPID 1380)**

- 05:14:35 / 05:14:35 — NtReadFile **[10 times]**
- 05:14:35 — VirtualProtectEx
- 05:14:35 / 05:14:36 — NtReadFile **[28 times]**
- 05:14:42 / 05:14:43 — MoveFileWithProgressW **[3 times]**
- 05:14:43 — RegSetValueExW
- 05:14:43 / 05:14:43 — NtReadFile **[14 times]**
- 05:14:44 — MoveFileWithProgress
- 05:14:44 / 05:14:44 — NtReadFile **[5 times]**
- 05:14:44 — Create Process
- 05:14:44 — Create Process

PID 1848

05:14:45 | Create Process | The malicious file created a child process as rundll32.exe **(PPID 2940)**

- 05:14:47 — InternetOpenW
- 05:14:50 / 05:14:51 — connect **[2 times]**

PID 3064

05:14:45 | Create Process | The malicious file created a child process as rundll32.exe **(PPID 2940)**

- 05:14:46 — Create Process

PID 2392

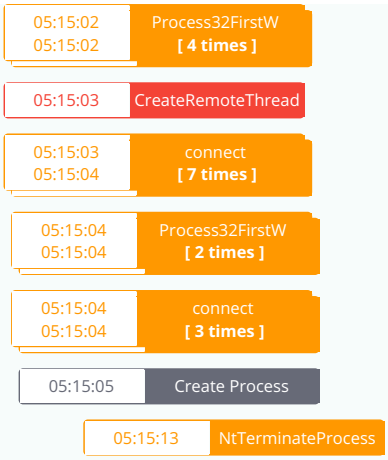
05:14:46 | Create Process | The malicious file created a child process as iexplore.exe **(PPID 3064)**

- 05:14:48 — NtSetInformationFile
- 05:14:49 — Create Process
- 05:15:02 / 05:15:02 — Process32FirstW **[2 times]**
- 05:15:19 — Create Process

PID 1708

05:14:49 | Create Process | The malicious file created a child process as iexplore.exe **(PPID 2392)**

- 05:14:54 — InternetOpenW
- 05:14:56 / 05:15:02 — connect **[25 times]**
- 05:15:02 / 05:15:02 — Process32FirstW **[3 times]**
- 05:15:02 — connect

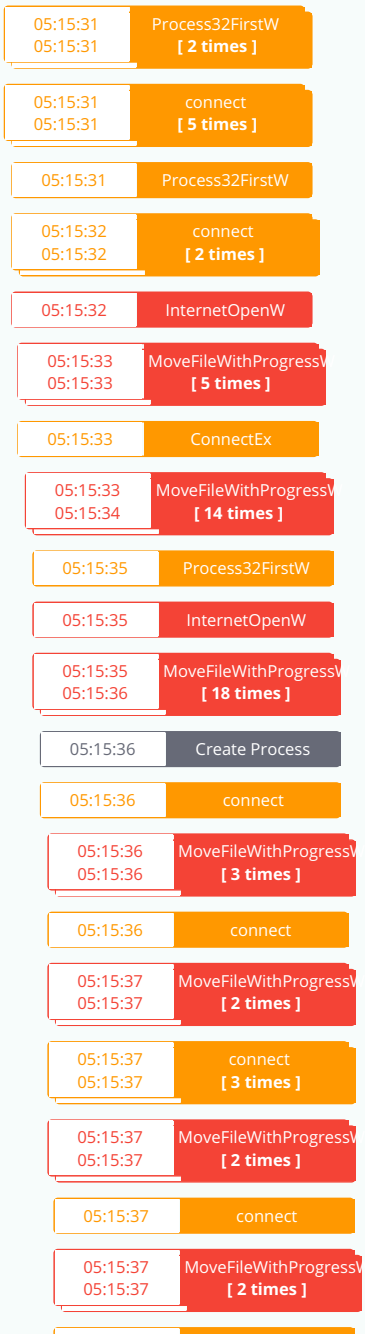


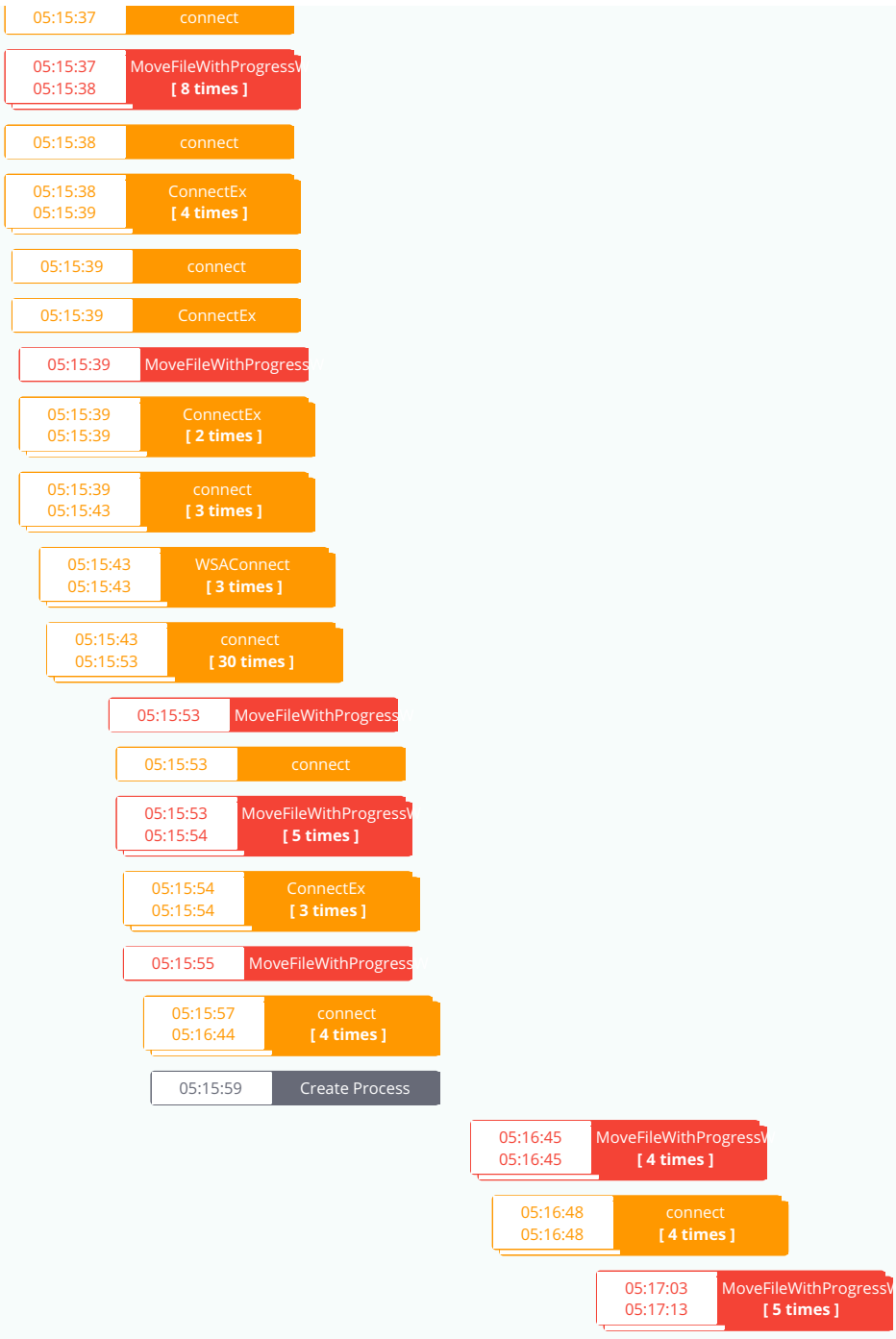
PID 2060

05:15:06 **Create Process** The malicious file created a child process as BitTorrentBar2ToolbarHelper.exe **(PPID 1708)**

PID 2252

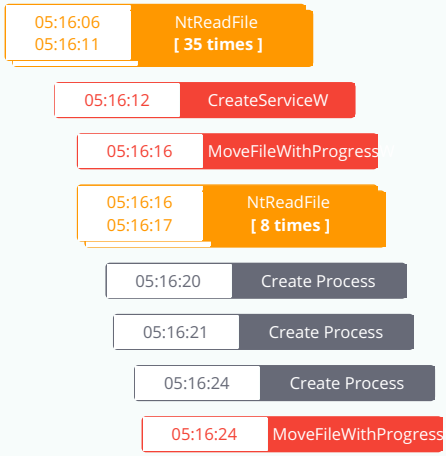
05:15:29 **Create Process** The malicious file created a child process as iexplore.exe **(PPID 2392)**





PID 504

05:16:06 **Create Process** The malicious file created a child process as BitTorrentBar2AutoUpdateHelper.exe **(PPID 2252)**



PID 2152

05:16:20 Create Process The malicious file created a child process as rundll32.exe **(PPID 504)**

05:16:20 Process32FirstW
05:16:22 NtReadFile
05:16:22 connect
05:16:22 05:16:22 Process32FirstW **[2 times]**

PID 2088

05:16:23 Create Process The malicious file created a child process as rundll32.exe **(PPID 504)**

05:16:24 Process32FirstW
05:16:24 RegSetValueExW
05:16:30 05:16:30 ConnectEx **[2 times]**

PID 2432

05:15:33 Create Process The malicious file created a child process as BitTorrentBar2ToolbarHelper.exe **(PPID 2252)**

PID 460

05:16:14 Create Process The malicious file created a child process as services.exe **(PPID 352)**

05:16:15 Create Process

PID 1764

05:16:15 Create Process The malicious file created a child process as ToolbarService.exe **(PPID 460)**

05:16:16 NtDelayExecution
05:16:17 ConnectEx

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\SHFOLDER.DLL
C:\Windows\System32\shfolder.dll
\??\MountPointManager
C:\Users\user\AppData\Local\Temp\
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\nse2858.tmp
C:\Users\user\AppData\Local\Temp\267ef53ea1a203e5181a3ab0d7ad860085834b19.exe
C:\Program Files (x86)
C:\Program Files (x86)\BitTorrentBar2
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\PublisherLogoDefault.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\setup_top.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\alerts_icon.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\truste_setup.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\search_icon.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\home_icon.bmp
C:\NUL
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\System.dll
C:
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\license.txt
C:\Users\user\AppData\Local\Temp\nsf28F7.tmp
C:\Users\user\AppData\Local\Temp\nsf28F7.tmp.tbBitT.dll
C:\Users\user\AppData\Local\Temp\RichEd20.DLL
C:\Windows\System32\riched20.dll
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\nsDialogs.dll
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\267ef53ea1a203e5181a3ab0d7ad860085834b19.exe.Local\

C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\license_uni.txt
C:\Users\user\AppData\Local\Temp\WSOCK32.dll
C:\Windows\System32\wsock32.dll
C:\Users\user\AppData\Local\Temp\MSIMG32.dll
C:\Windows\System32\msimg32.dll
C:\Users\user\AppData\Local\Temp\WINMM.dll
C:\Windows\System32\winmm.dll
C:\Users\user\AppData\Local\Temp\DNSAPI.dll
C:\Windows\System32\dnsapi.dll
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Users\user\AppData\LocalLow
C:\Users\user\AppData\LocalLow\Temp\Logs
C:\Users\user\AppData\LocalLow\Temp
C:\Program Files (x86)\BitTorrentBar2\tbBitT.dll
C:\Program Files (x86)\BitTorrentBar2\prxtbBitT.dll
C:\Program Files (x86)\BitTorrentBar2\ldrtbBitT.dll
C:\Program Files (x86)\BitTorrentBar2\uninstall.dat
C:\Program Files (x86)\BitTorrentBar2\0
C:\Program Files (x86)\BitTorrentBar2\toolbar.cfg
C:\Users\user\AppData\Local\Conduit
C:\Users\user\AppData\Local\Conduit\CT3045275
C:\Program Files (x86)\BitTorrentBar2\BitTorrentBar2ToolbarHelper.exe
C:\Users\user\AppData\Local\Conduit\CT3045275\BitTorrentBar2AutoUpdateHelper.exe
C:\Program Files (x86)\BitTorrentBar2\GottenAppsContextMenu.xml
C:\Program Files (x86)\BitTorrentBar2\OtherAppsContextMenu.xml
C:\Program Files (x86)\BitTorrentBar2\SharedAppsContextMenu.xml
C:\Program Files (x86)\BitTorrentBar2\ToolbarContextMenu.xml
C:\Program Files (x86)\BitTorrentBar2\uninstall.exe
C:\Users\user\AppData\LocalLow\BitTorrentBar2\tbBitT.dll
C:\Users\user\AppData\LocalLow\BitTorrentBar2
C:\Users\user\AppData\LocalLow\BitTorrentBar2\ldrtbBitT.dll

C:\Users\user\AppData\LocalLow\BitTorrentBar2\toolbar.cfg
C:\Users\user\AppData\LocalLow\BitTorrentBar2\Logs
C:\Program Files (x86)\Conduit
C:\Users\user\AppData\LocalLow\conduit
C:\Users\user\AppData\LocalLow\BitTorrentBar2\INSTALL.LOG
C:\Users\user\AppData\LocalLow\BitTorrentBar2\ReferenceCookie.txt
C:\Windows\SysWOW64\wininet.dll
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\desktop.ini

READ REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Version
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Local AppData
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\MultiCommunityEnabled
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\ComId
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_CURRENT_USER\Control Panel\Desktop\SmoothScroll
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\EnableBalloonTips
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewAlphaSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewShadow
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AccListViewV6
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\UseDoubleClickTimer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\LastLoggedOnUser
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\LastLoggedOnSAMUser
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Enable Browser Extensions
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Use Search Asst
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes\DefaultScope
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\Enable Browser Extensions
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\Use Search Asst
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\ToolbarDllName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\ToolbarDllName
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\LoaderDllName

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\LoaderDllName
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Log\LogFileMaxSize
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\PlatformType
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\PlatformType
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Conduit\Platforms\{656461ef-40f6-4115-9ff1-bced9812ccbb}\HostID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Conduit\Platforms\{656461ef-40f6-4115-9ff1-bced9812ccbb}\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\HostID
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Log\LogLevelsString
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Monitored\MultiCommunityEnabled
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\MultiCommunityEnabled
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Monitored\GroupingEnabled
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\GroupingEnabled
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\GroupingEnabled
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Monitored\SponsorId
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\SponsorId
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Monitored\MultiCommunityID
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Monitored\SHRINK_TOOLBAR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\ProxyDllPath
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\DisplayName

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\PublisherLogoDefault.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\setup_top.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\alerts_icon.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\truste_setup.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\search_icon.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\home_icon.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\System.dll
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\license.txt
C:\Users\user\AppData\Local\Temp\nsf28F7.tmp.tbBitT.dll
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\nsDialogs.dll
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\license_uni.txt
C:\Program Files (x86)\BitTorrentBar2\toolbar.cfg
C:\Program Files (x86)\BitTorrentBar2\BitTorrentBar2ToolbarHelper.exe
C:\Users\user\AppData\Local\Conduit\CT3045275\BitTorrentBar2AutoUpdateHelper.exe

C:\Program Files (x86)\BitTorrentBar2\tbBitT.dll

C:\Program Files (x86)\BitTorrentBar2\prxtbBitT.dll

C:\Program Files (x86)\BitTorrentBar2\ldrtbBitT.dll

C:\Program Files (x86)\BitTorrentBar2\GottenAppsContextMenu.xml

C:\Program Files (x86)\BitTorrentBar2\OtherAppsContextMenu.xml

C:\Program Files (x86)\BitTorrentBar2\SharedAppsContextMenu.xml

C:\Program Files (x86)\BitTorrentBar2\ToolbarContextMenu.xml

C:\Program Files (x86)\BitTorrentBar2\uninstall.exe

C:\Users\user\AppData\LocalLow\BitTorrentBar2\tbBitT.dll

C:\Users\user\AppData\LocalLow\BitTorrentBar2\ldrtbBitT.dll

C:\Users\user\AppData\LocalLow\BitTorrentBar2\toolbar.cfg

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat

C:\Program Files (x86)\Conduit\Community Alerts\Alert.dll

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\ToolbarUsage[1].ashx

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\Toolbar[1].txt

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{6FE1609A-3EC0-11E8-9C49-080027CB305F}.dat

C:\Users\user\AppData\Local\Temp\~DF249917161D470F92.TMP

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6FE1609B-3EC0-11E8-9C49-080027CB305F}.dat

C:\Users\user\AppData\Local\Temp\~DFF763592DAA797801.TMP

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{884B39D2-3EC0-11E8-9C49-080027CB305F}.dat

C:\Users\user\AppData\Local\Temp\~DFA75DB6A4DFBEDD61.TMP

C:\Users\user\AppData\Local\Microsoft\Feeds Cache\index.dat

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\install-complete[1].htm

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\grid[1].css

C:\Users\user\AppData\Roaming\Microsoft\Windows\PrivacIE\index.dat

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\jquery.smartbanner[1].js

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\css[1].txt

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\font-awesome[1].css

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\jquery.smartbanner[1].css

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\panels[1].css

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\frog[1].css

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\animate-custom[1].css

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\animate-custom[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\fontawesome-webfont[1].eot
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\mem8YaGs126MiZpBA-U1Uw[1].eot
\??\pipe\GadgetsManagerPipeServerCT3045275_HIGH
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\ToolbarUsage[1].ashx
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\jquery.min[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\gpt[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\detection[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\jquery.smartbanner[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\f[1].txt
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\clientlog_users_conduit_com[1].txt
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\CT3045275[1].txt
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\appsmetadata_toolbar_conduit-services_com[1].txt
C:\Users\user\AppData\Local\Temp\151161009936386753.tmp
C:\Users\user\AppData\LocalLow\BitTorrentBar2\Repository\conduit_CT3045275_CT3045275\AppsMetaData\data.txt
C:\Users\user\AppData\Local\Temp\359066060236388636.tmp
C:\Users\user\AppData\LocalLow\BitTorrentBar2\Repository\conduit_CT3045275_CT3045275\ToolbarSettings\data.txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@search.conduit[1].txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@search.conduit[2].txt
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\50136351[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\respond.min[1].js
C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_75_304_CT3045275_Images_634220815653506250_png.png.tmp
C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_75_304_CT3045275_Images_634220815653506250_png.png
C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_searchengines_go_btn_new_gif.gif.tmp
C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_MarketPlace_93_ce3_93951332-f9a7-4af7-af02-17ec3d749ce3_Appearance_634159521796627506_24x24_png.png.tmp
C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_92_279_CT2790392_Images_634220879921318750_png.png.tmp
C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_searchengines_go_btn_new_gif.gif

RESOLVED APIS

cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
shfolder.dll.SHGetFolderPathW
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
setupapi.dll.CM_Get_Device_Interface_List_ExW

kernel32.dll.GetUserDefaultUILanguage
system.dll.Call
kernel32.dll.GetDiskFreeSpaceExW
system.dll.Int64Op
dwmapi.dll.DwmIsCompositionEnabled
comctl32.dll.RegisterClassNameW
uxtheme.dll.EnableThemeDialogTexture
uxtheme.dll.OpenThemeData
uxtheme.dll.GetThemeBool
ole32.dll.CoInitializeEx
ole32.dll.CoUninitialize
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoRevokeInitializeSpy
nsdialogs.dll.Create
nsdialogs.dll.SetRTL
nsdialogs.dll.CreateControl
user32.dll.LoadImageW
imm32.dll.ImmGetContext
imm32.dll.ImmReleaseContext
imm32.dll.ImmAssociateContext
imm32.dll.ImmIsIME
comctl32.dll.HIMAGELIST_QueryInterface
comctl32.dll.DrawShadowText
comctl32.dll.DrawSizeBox
comctl32.dll.DrawScrollBar
comctl32.dll.SizeBoxHwnd
comctl32.dll.ScrollBar_MouseMove
comctl32.dll.ScrollBar_Menu
comctl32.dll.HandleScrollCmd
comctl32.dll.DetachScrollBars
comctl32.dll.AttachScrollBars
comctl32.dll.CCSetScrollInfo
comctl32.dll.CCGetScrollInfo
comctl32.dll.CCEnableScrollBar
comctl32.dll.QuerySystemGestureStatus

uxtheme.dll.#49
uxtheme.dll.CloseThemeData
uxtheme.dll.DrawThemeBackground
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryValueExW
advapi32.dll.RegCloseKey
gdi32.dll.GetFontAssocStatus
advapi32.dll.RegQueryValueExA
advapi32.dll.RegQueryInfoKeyW
advapi32.dll.RegEnumKeyExW
gdi32.dll.GetTextFaceAliasW
gdi32.dll.GetTextExtentExPointWPri
advapi32.dll.RegEnumValueW
kernel32.dll.GetFileSize
system.dll.Alloc
kernel32.dll.ReadFile
system.dll.Free
nsdialogs.dll.OnClick
nsdialogs.dll.Show
gdi32.dll.GdiIsMetaPrintDC
uxtheme.dll.BufferedPaintInit
uxtheme.dll.BufferedPaintRenderAnimation
uxtheme.dll.BeginBufferedAnimation
uxtheme.dll.IsThemeBackgroundPartiallyTransparent
uxtheme.dll.DrawThemeParentBackground
uxtheme.dll.GetThemeBackgroundContentRect
uxtheme.dll.DrawThemeText
uxtheme.dll.EndBufferedAnimation
uxtheme.dll.GetThemePartSize
uxtheme.dll.GetThemeTextExtent
uxtheme.dll.GetThemeMargins
uxtheme.dll.DrawThemeParentBackgroundEx

DELETED FILES

C:\Users\user\AppData\Local\Temp\nse2858.tmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp
C:\Users\user\AppData\Local\Temp\nsf28F7.tmp.tbBitT.dll
C:\Program Files (x86)\BitTorrentBar2\
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\alerts_icon.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\home_icon.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\license.txt
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\license_uni.txt
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\nsDialogs.dll
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\PublisherLogoDefault.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\search_icon.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\setup_top.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\System.dll
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\truste_setup.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\ToolbarUsage[1].ashx
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\font-awesome[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\grid[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\css[1].txt
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\jquery.smartbanner[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\jquery.smartbanner[1].css
C:\Users\user\AppData\Local\Temp\339705145836385539.tmp
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\clientlog_users_conduit_com[1].txt
C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_75_304_CT3045275_Images_634220815653506250_png.png.tmp
C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_searchengines_go_btn_new_gif.gif.tmp
C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_MarketPlace_93_ce3_93951332-f9a7-4af7-af02-17ec3d749ce3_Appearance_634159521796627506_24x24_png.png.tmp
C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_92_279_CT2790392_Images_634220879921318750_png.png.tmp
C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_75_304_CT3045275_images_634818561434829991_24PX_png.png.tmp
C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_75_304_CT3045275_Images_634225281783662500_png.png.tmp
C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_92_279_CT2790392_Images_634225278165850000_png.png.tmp
C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_92_279_CT2790392_Images_634225280526593750_png.png.tmp
C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_92_279_CT2790392_Images_634225279692725000_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_92_279_CT2790392_Images_634225284881631250_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_92_279_CT2790392_Images_634225280643975000_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_92_279_CT2790392_Images_634225284383662500_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_92_279_CT2790392_Images_634225280304131250_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_92_279_CT2790392_Images_634225281436162500_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_92_279_CT2790392_Images_634225287181631250_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_92_279_CT2790392_Images_634225279948156250_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_92_279_CT2790392_Images_634225287547412500_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_75_304_CT3045275_Images_634226713903631250_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_75_304_CT3045275_Images_634244833256762500_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\ExternalComponent\http___contextmenu_toolbar_conduit-services_com__name=SharedApps&locale=EB_LOCALE&ctid=CT3045275.xml.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\ExternalComponent\http___contextmenu_toolbar_conduit-services_com__name=Toolbar&locale=EB_LOCALE&ctid=CT3045275&UM=UM_UNINSTALL_ID.xml.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_searchengines_search_icon_gif.gif.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_SearchEngines_video_gif.gif.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\ExternalComponent\http___contextmenu_toolbar_conduit-services_com__name=OtherApps&locale=EB_LOCALE&ctid=CT3045275.xml.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_SearchEngines_images_search_gif.gif.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\ExternalComponent\http___contextmenu_toolbar_conduit-services_com__name=GottenApps&locale=EB_LOCALE&ctid=CT3045275.xml.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_SearchEngines_tfd_gif.gif.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_bankImages_ConduitEngine_ContextMenu_LikeIcon_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_SearchEngines_news_icon_gif.gif.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_searchengines_softonic_gif.gif.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_main_menu_help_gif.gif.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_main_menu_upgrade_gif.gif.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_eula_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_main_menu_contact_gif.gif.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_main_menu_about_gif.gif.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_main_menu_home_page_gif.gif.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_main_menu_privacy_gif.gif.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_main_menu_clear_history_gif.gif.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_main_menu_shrink_gif.gif.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_main_menu_options_gif.gif.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_main_menu_refresh_gif.gif.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_stgbssint_com_images_Menu_uninstall-icon_png.png.tmp

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@search.conduit[1].txt

C:\Users\user\AppData\LocalLow\BitTorrentBar2\Rss\http___rss_cnn_com_rss_cnn_latest_rss.xml.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_Conduit_com_bankImages_ConduitEngine_ContextMenu_More_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_Conduit_com_bankImages_ConduitEngine_ContextMenu_Browse_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_Conduit_com_bankImages_ConduitEngine_ContextMenu_Upgrade_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_Conduit_com_bankImages_ConduitEngine_ContextMenu_LikeIcon_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_Conduit_com_bankImages_ConduitEngine_ContextMenu_Refresh_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\plugins\{5E1360DC-8FA8-40df-A8CD-FC3831B3634B}\{5E1360DC-8FA8-40df-A8CD-FC3831B3634B}.cpi

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_Conduit_com_bankImages_ConduitEngine_ContextMenu_Options_png.png.tmp

C:\Users\user\AppData\LocalLow\BitTorrentBar2\CacheIcons\http___storage_Conduit_com_bankImages_ConduitEngine_ContextMenu_Hide_png.png.tmp

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\weatherrequest[1].xml

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL

HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\SendDWUsage

HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\SendBHOUsage

HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\ConduitShowToolbarCloseButton

HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\Update\CurrentlyRunning

HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\Update\IsNotificationNeeded

REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_CLASSES_ROOT\CLSID\{30F9B915-B755-4826-820B-08FBA6BD249D}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Version
HKEY_LOCAL_MACHINE\SOFTWARE\BitTorrentBar2\toolbar
HKEY_CLASSES_ROOT\CLSID\{656461ef-40f6-4115-9ff1-bced9812ccbb}\InprocServer32
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Local AppData
HKEY_LOCAL_MACHINE\Software\BitTorrentBar2\toolbar
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\MarkOldApps
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\MultiCommunityEnabled
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\ComId
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\267ef53ea1a203e5181a3ab0d7ad860085834b19.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\System
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\MS Shell Dlg 2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\MS Shell Dlg
HKEY_CURRENT_USER
HKEY_CURRENT_USER\Control Panel\Desktop
HKEY_CURRENT_USER\Control Panel\Desktop\SmoothScroll
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\EnableBalloonTips
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewAlphaSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewShadow
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AccListViewV6
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\UseDoubleClickTimer

EXECUTED COMMANDS

rundll32 "C:\Program Files (x86)\BitTorrentBar2\tbBitT.dll" DllSendInstallationUsage New Installation
rundll32 "C:\Program Files (x86)\BitTorrentBar2\tbBitT.dll" DllRunIEMediumIntegrity
C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE http://BitTorrentBar2.OurToolbar.com/SetupFinish
"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:2392 CREDAT:79873
"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:2392 CREDAT:14339
C:\Program Files (x86)\BitTorrentBar2\BitTorrentBar2ToolbarHelper.exe DllRun "C:\Users\user\AppData\LocalLow\BitTorrentBar2\tbBitT.dll" DllCleanEnableExtensionDoing
rundll32.exe "C:\Users\user\AppData\LocalLow\BitTorrentBar2\tbBitT.dll" DllWriteSocialCookies
C:\Users\user\AppData\Local\Conduit\CT3045275\BitTorrentBar2AutoUpdateHelper.exe /S -userdir="C:\Users\user\AppData\LocalLow" -toolbarname="BitTorrentBar2" -dllname="tbBit0.dll" -proxydllname="prxtbBit0.dll" -loaderdllname="ldrtbBit0.dll" -helpername="BitTorrentBar2ToolbarHelper1.exe" -hostid="{656461ef-40f6-4115-9ff1-bced9812ccbb}" -mystuffenabled="TRUE" -highintegrity
rundll32.exe "C:\Users\user\AppData\LocalLow\BitTorrentBar2\tbBit0.dll" DllWriteSocialCookies
C:\Windows\system32\rundll32.exe "C:\Users\user\AppData\LocalLow\BitTorrentBar2\prxtbBit0.dll" DllOnUpdateFinish
"C:\Windows\SysWOW64\Rundll32.exe" "C:\Users\user\AppData\Local\Conduit\BackgroundContainer\BackgroundContainer.dll",DllRun
C:\Program Files (x86)\Tbccint\ToolbarService\ToolbarService.exe

READ FILES

\Device\KsecDD
C:\Windows\System32\shfolder.dll
C:\Users\user\AppData\Local\Temp\nse2858.tmp
C:\Users\user\AppData\Local\Temp\267ef53ea1a203e5181a3ab0d7ad860085834b19.exe
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\System.dll
C:\Users\user\AppData\Local\Temp\nsf28F7.tmp
C:\Windows\System32\riched20.dll
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\nsDialogs.dll
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\PublisherLogoDefault.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\setup_top.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\search_icon.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\alerts_icon.bmp
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\home_icon.bmp
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\license.txt
C:\Users\user\AppData\Local\Temp\nsu28B7.tmp\license_uni.txt

C:\Users\user\AppData\Local\Temp\nsf28F7.tmp.tbBitT.dll
C:\Windows\System32\wsock32.dll
C:\Windows\System32\msimg32.dll
C:\Windows\System32\winmm.dll
C:\Windows\System32\dnsapi.dll
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Program Files (x86)\BitTorrentBar2\prxtbBitT.dll
C:\Program Files (x86)\BitTorrentBar2\toolbar.cfg
C:\Program Files (x86)\BitTorrentBar2\tbBitT.dll
C:\Program Files (x86)\BitTorrentBar2\ldrtbBitT.dll
C:\Users\user\AppData\LocalLow\BitTorrentBar2\ldrtbBitT.dll
C:\Users\user\AppData\LocalLow\BitTorrentBar2\tbBitT.dll
C:\Users\user\AppData\LocalLow\BitTorrentBar2\INSTALL.LOG
C:\Windows\SysWOW64\wininet.dll
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Windows\System32\IPHLPAPI.DLL
C:\Windows\System32\winnsi.dll
C:\Users\user\AppData\LocalLow\BitTorrentBar2\toolbar.cfg
C:\Program Files (x86)\Conduit\Community Alerts\Alert.dll
C:\Program Files (x86)\BitTorrentBar2\tbBitT.dll.123.Manifest
C:\Program Files (x86)\BitTorrentBar2\tbBitT.dll.124.Manifest
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Program Files (x86)\Internet Explorer\sqmapi.dll
C:\Sessions\1\BaseNamedObjects\Isolation Signal Registry (6FE16098-3EC0-11E8-9C49-080027CB305F, 0)
C:\Windows\SysWOW64\shell32.dll
C:\Users\user\AppData\Local\Temp\Low
C:\Program Files (x86)\Internet Explorer\ieproxy.dll
C:\Windows\System32\url.dll
C:\Program Files (x86)\Microsoft Office\Office12\REFBAR.ICO
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{6FE1609A-3EC0-11E8-9C49-080027CB305F}.dat
C:\Users\user\AppData\Local\Temp\~DF249917161D470F92.TMP
C:\Windows\SysWOW64\ieframe.dll

C:\Windows\SysWOW64\stdole2.tlb
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6FE1609B-3EC0-11E8-9C49-080027CB305F}.dat
C:\Users\user\AppData\Local\Temp\~DFF763592DAA797801.TMP
C:\
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004a.db
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\Favorites\desktop.ini
C:\Users\user\Desktop\desktop.ini
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{884B39D2-3EC0-11E8-9C49-080027CB305F}.dat
C:\Users\user\AppData\Local\Temp\~DFA75DB6A4DFBEDD61.TMP
C:\Windows\System32\imageres.dll
C:\Program Files (x86)\Internet Explorer\IEShims.dll
C:\Users\user\AppData\Local\Microsoft\Feeds Cache\index.dat
C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll
C:\Windows\AppPatch\sysmain.sdb
C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\
C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll
C:\Program Files (x86)\BitTorrentBar2\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll

MUTEXES

CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
CONDUIT_SHARED_MUTEX
Local\LRIEElevationPolicyMutex
Local_!MSFTHISTORY!_
Local\c:!users!user!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Local\c:!users!user!appdata!roaming!microsoft!windows!cookies!
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!
Local\WininetStartupMutex
Local\WininetConnectionMutex
Local\WininetProxyRegistryMutex

Local\ZonesCounterMutex
Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
Local\!IETld!Mutex
CCommunicatorLogicMutex_
IESQMMUTEX_0_208
CCommunicatorLogicMutex_CT3045275
Local\!BrowserEmulation!SharedMemory!Mutex
ConnHashTable<2392>_HashTable_Mutex
ToolbarInjectionDoneAlreadyMutexName2392
API_HOOK_MUTES_2392
AboutTabsIE9Mutex
InitIEMenuHooks_Mutex_2392
Local\c:!users!user!appdata!local!microsoft!feeds cache!
Local\c:!users!user!appdata!roaming!microsoft!windows!privacie!
InitIEMenuHooks_Mutex_1708
API_HOOK_MUTES_1708
EI_Conduit_Social_Cookie_Mutex_CT30452754
TryToInjectToIe2392
EI_InitFromDefaultDataIfNeeded
ConduitGadgetsMgrMutex_CT3045275_HIGH
EI_3rdParty_MutexCT3045275
http://contextmenu.toolbar.conduit-services.com/?name=Toolbar&locale=EB_LOCALE&ctid=CT3045275&UM=UM_UNINSTALL_ID
http://contextmenu.toolbar.conduit-services.com/?name=SharedApps&locale=EB_LOCALE&ctid=CT3045275
http://contextmenu.toolbar.conduit-services.com/?name=GottenApps&locale=EB_LOCALE&ctid=CT3045275
http://contextmenu.toolbar.conduit-services.com/?name=OtherApps&locale=EB_LOCALE&ctid=CT3045275
InitIEMenuHooks_Mutex_2252
API_HOOK_MUTES_2252
EI_Plugin_Download_CT3045275_{5E1360DC-8FA8-40df-A8CD-FC3831B3634B}
PRICE_GONG_SETTINGS_LOAD_MUTEX
PRICE_GONG_CONFIG_FILE_LOAD_MUTEX
PRICE_FACTOR_INIT_MRU_MUTEX
!SHMSFTHISTORY!
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!mshist012018041320180414!

DBWinMutex
{1B655094-FE2A-433c-A877-FF9793445069}
Local\c:!users!user!appdata!roaming!microsoft!windows!ietldcache!
MSIMGSIZECacheMutex
Community Alerts
EI_Toolbar_Update_Mutex_CT3045275_Update
SendClientErrorLogs
http://contextmenu.toolbar.conduit-services.com/?name=Toolbar&locale=en&ctid=CT3045275&UM=UM_UNINSTALL_ID
http://contextmenu.toolbar.conduit-services.com/?name=SharedApps&locale=en&ctid=CT3045275
http://contextmenu.toolbar.conduit-services.com/?name=GottenApps&locale=en&ctid=CT3045275
http://contextmenu.toolbar.conduit-services.com/?name=OtherApps&locale=en&ctid=CT3045275
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!mshist012018041420180415!
BROKER_HELP_MUTEX_CONDUIT_SHARED_MUTEX
BROKER_HELP_MUTEX_TOOLBAR_SERVICE_INSTALL_MUTEX
TOOLBAR_SERVICE_INSTALL_MUTEX
BROKER_HELP_MUTEX_UpdateHookDllPathAndVersion
UpdateHookDllPathAndVersion
SessionHomepageProtectionDisabledMutexName
SessionSearchProtectionDisabledMutexName
Conduit_Alert_Autoupdate_Mutex
BackgroundContainerProcessRunOnce
BackgroundContainerProcessRunOnceV2

MODIFIED REGISTRY KEYS

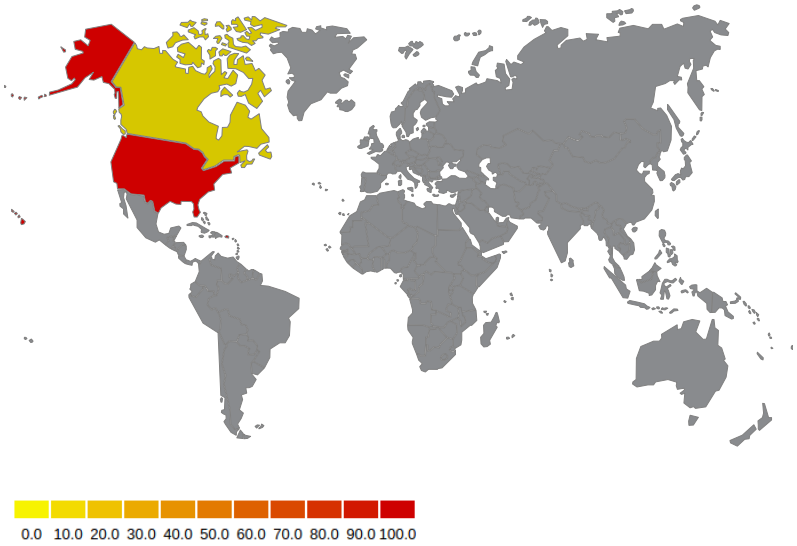
HKEY_LOCAL_MACHINE\Software\BitTorrentBar2\toolbar
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\MarkOldApps
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\GroupingServerURL
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\SearchServerUrl
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Server
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\ShouldPerformGroupByOS
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\UsageURL
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\WebServerUrl
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Write us link
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\ShouldCheckEnableAlerts

HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\IE5
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\IE5\CabinetVisible
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\IE5\ExplorerVisible
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\IE5\FirstTime
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\IE5\Visible
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\EnableSearchFromAddress
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\FixPageNotFoundError
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\SearchFromAddressUrl
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\OpenSetupFinishPage
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\ImportFromNotDUP
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\ShouldSendReferalCookie
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\FeatureProtector
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\FeatureProtector\NotifyOfSettingsChange
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\FeatureProtector\HomePage
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\FeatureProtector\HomePage\HPProtectCount
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\FeatureProtector\BrowserSearch
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\FeatureProtector\BrowserSearch\DSProtectCount
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\FeatureProtector\SendProtectorDataViaLogin
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Enable Browser Extensions
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Use Search Asst
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\URLSearchHooks\{656461ef-40f6-4115-9ff1-bced9812ccbb}
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\settings\MyStuff
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\MyStuff\StagingEnable
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Monitored
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Monitored\SHRINK_TOOLBAR
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\settings\RadioPlayer
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\RadioPlayer\ShrinkState
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\URLSearchHooks
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\URLSearchHooks\{656461ef-40f6-4115-9ff1-bced9812ccbb}
HKEY_CURRENT_USER\Software\AppDataLow\Software\Conduit\RevertSettings
HKEY_CURRENT_USER\Software\AppDataLow\Software\Conduit\RevertSettings\HomePage
HKEY_CURRENT_USER\Software\AppDataLow\Software\Conduit\RevertSettings\DefaultSearchScope
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\BrowserSearchURL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\BrowserSearchDisplayName

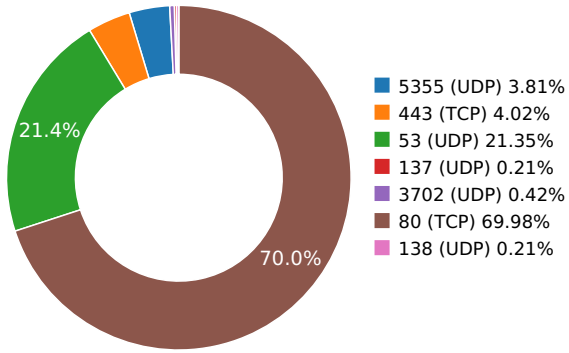
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\SearchScopes\{afdbddaa-5d3f-42ee-b79c-185a7020515b}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\SearchScopes\{afdbddaa-5d3f-42ee-b79c-185a7020515b}\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\SearchScopes\{afdbddaa-5d3f-42ee-b79c-185a7020515b}\URL
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes\{afdbddaa-5d3f-42ee-b79c-185a7020515b}
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes\{afdbddaa-5d3f-42ee-b79c-185a7020515b}\DisplayName
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes\{afdbddaa-5d3f-42ee-b79c-185a7020515b}\URL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\SearchScopes\DefaultScope
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes\DefaultScope
HKEY_CURRENT_USER\Software\AppDataLow\Software\ConduitSearchScopes
HKEY_CURRENT_USER\Software\AppDataLow\Software\ConduitSearchScopes\{afdbddaa-5d3f-42ee-b79c-185a7020515b}
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\FeatureProtector\BrowserSearch\DSInstall
HKEY_CURRENT_USER\Software\AppDataLow\Software\BitTorrentBar2\toolbar\Settings\FeatureProtector\HomePage\HPInstall
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\ComId
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\ToolbarAPIComId
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\FindBarComId
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\DisplayTitle
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\GroupingEnabled
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\InstallationId
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\InstallationType
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\MultiCommunityEnabled
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\Path
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\Server
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\ShouldPerformGroupByOS
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\ShouldShowPersonalComponentDlg
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\SponsorId
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\ToolbarHelperFileName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\PlatformType
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BitTorrentBar2\toolbar\IsEngineHost

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	8.8.8.8	United States	15169	Level 3 Parent, LLC	Malware Process
	104.106.251.24	United States	16625	Akamai Technologies, Inc.	Malware Process
	172.217.10.66	United States	15169	Google LLC	Malware Process
	172.217.10.67	United States	15169	Google LLC	Malware Process
	172.217.12.194	United States	15169	Google LLC	Malware Process
	172.217.12.202	United States	15169	Google LLC	Malware Process
	172.217.3.110	United States	15169	Google LLC	Malware Process
	172.217.6.226	United States	15169	Google LLC	Malware Process
	172.217.6.238	United States	15169	Google LLC	Malware Process
	18.216.93.150	United States	16509	Amazon Technologies Inc.	Malware Process
	184.26.44.104	United States	20940	Akamai Technologies, Inc.	Malware Process
	184.26.44.106	United States	20940	Akamai Technologies, Inc.	Malware Process
	184.26.44.97	United States	20940	Akamai Technologies, Inc.	OS Process
	184.26.44.98	United States	20940	Akamai Technologies, Inc.	OS Process
	23.4.187.27	United States	16625	Akamai Technologies, Inc.	Malware Process
	23.50.229.108	United States	16625	Akamai Technologies, Inc.	Malware Process
	23.67.250.112	United States	20940	Akamai Technologies, Inc.	Malware Process
	23.67.250.138	United States	20940	Akamai Technologies, Inc.	Malware Process
	23.67.250.96	United States	20940	Akamai Technologies, Inc.	Malware Process
	34.198.95.87	United States	14618	Amazon Technologies Inc.	Malware Process
	52.216.229.99	United States	16509	Amazon Technologies Inc.	Malware Process
	52.216.86.35	United States	16509	Amazon Technologies Inc.	Malware Process

Name	IP	Country	ASN	ASN Name	Trigger Process Type
	54.231.49.234	United States	16509	Amazon.com, Inc.	Malware Process
	66.150.118.61	United States	10913	Internap Network Services Corpor...	Malware Process
	69.28.187.228	United States	22822	Limelight Networks, Inc.	Malware Process
	72.246.43.9	Canada	20940	Akamai Technologies, Inc.	Malware Process
	72.30.35.9	United States	26101	Inktomi Corporation	Malware Process
	74.6.144.137	United States	26101	Inktomi Corporation	Malware Process
	52.85.101.89	United States	16509	Amazon Technologies Inc.	Malware Process
	52.216.101.21	United States	16509	Amazon Technologies Inc.	Malware Process
	23.50.230.12	United States	16625	Akamai Technologies, Inc.	Malware Process
	104.31.74.124		13335	Cloudflare, Inc.	Malware Process
	23.67.250.107		20940	Akamai Technologies, Inc.	Malware Process
	172.217.10.35		15169	Google LLC	Malware Process
	195.78.120.93		56473		Malware Process
	54.235.180.144		14618	Amazon.com, Inc.	Malware Process
	104.107.37.144		16625	Akamai Technologies, Inc.	Malware Process
	18.217.188.215		16509	Amazon Technologies Inc.	Malware Process
	72.246.43.51		20940	Akamai Technologies, Inc.	Malware Process
	23.67.250.115		20940	Akamai Technologies, Inc.	Malware Process
	173.194.68.82		15169	Google LLC	Malware Process
	72.30.35.10		26101	Inktomi Corporation	Malware Process
	195.78.120.79		56473		Malware Process
	173.222.184.25		16625	Akamai Technologies, Inc.	Malware Process
	98.136.96.140		36646	Yahoo! Inc.	Malware Process
	23.200.109.88		20940	Akamai Technologies, Inc.	Malware Process
	104.107.32.194		16625	Akamai Technologies, Inc.	Malware Process
	98.136.96.140		36646	Yahoo! Inc.	Malware Process
	172.217.10.51		15169	Google LLC	Malware Process
	104.107.50.14		16625	Akamai Technologies, Inc.	Malware Process
	52.216.163.53		16509	Amazon Technologies Inc.	Malware Process
	205.185.216.10		20446	Highwinds Network Group, Inc.	Malware Process
	195.78.120.104		56473		Malware Process
	23.200.109.88		20940	Akamai Technologies, Inc.	Malware Process
	195.78.120.83		56473		Malware Process
	199.101.114.106		56473	Conduit USA, Inc.	Malware Process
	54.243.137.87		14618	Amazon Technologies Inc.	Malware Process
	23.67.250.121		20940	Akamai Technologies, Inc.	Malware Process
	184.24.97.174		20940	Akamai Technologies, Inc.	OS Process

Name	IP	Country	ASN	ASN Name	Trigger Process Type
	172.217.10.51		15169	Google LLC	Malware Process
	172.217.10.227		15169	Google LLC	Malware Process
	52.216.130.11		16509	Amazon Technologies Inc.	Malware Process
	195.78.120.79		56473		Malware Process
	184.24.97.159		20940	Akamai Technologies, Inc.	OS Process
	82.163.248.194		199391		Malware Process
	172.217.10.78		15169	Google LLC	Malware Process
	195.78.120.182		56473		Malware Process
	172.217.10.238		15169	Google LLC	Malware Process
	23.67.250.120		20940	Akamai Technologies, Inc.	Malware Process
	195.78.120.73		56473		Malware Process
	172.217.10.130		15169	Google LLC	Malware Process
	66.135.34.17		13768	ServerBeach	Malware Process
	23.67.250.19		20940	Akamai Technologies, Inc.	Malware Process
	104.107.44.23		16625	Akamai Technologies, Inc.	Malware Process
	195.78.120.80		56473		Malware Process
	23.67.251.19		20940	Akamai Technologies, Inc.	Malware Process
	172.217.10.226		15169	Google LLC	Malware Process
	172.217.10.42		15169	Google LLC	Malware Process
	172.217.10.234		15169	Google LLC	Malware Process
	72.246.43.51		20940	Akamai Technologies, Inc.	Malware Process
	195.78.120.65		56473		Malware Process
	195.78.120.102		56473		Malware Process
	199.101.114.130		56473	Conduit USA, Inc.	Malware Process
	172.217.12.130		15169	Google LLC	Malware Process
	104.107.32.194		16625	Akamai Technologies, Inc.	Malware Process
	93.184.216.182		15133		Malware Process
	199.101.114.251		56473	Conduit USA, Inc.	Malware Process
	23.67.250.24		20940	Akamai Technologies, Inc.	Malware Process
	172.217.7.2		15169	Google LLC	Malware Process
	72.5.205.38		19024	Internap Network Services Corpor...	Malware Process
	172.217.10.238		15169	Google LLC	Malware Process
	199.101.115.202		56473	Conduit USA, Inc.	Malware Process
	208.111.178.227		22822	Limelight Networks, Inc.	Malware Process
	104.17.28.15		13335	Cloudflare, Inc.	Malware Process
	199.101.114.100		56473	Conduit USA, Inc.	Malware Process
	195.78.120.65		56473		Malware Process

Name	IP	Country	ASN	ASN Name	Trigger Process Type
	172.217.10.46		15169	Google LLC	Malware Process
	195.78.120.83		56473		Malware Process
	195.78.120.80		56473		Malware Process
	23.67.250.128		20940	Akamai Technologies, Inc.	Malware Process
	172.217.10.142		15169	Google LLC	Malware Process
	52.85.101.234		16509	Amazon Technologies Inc.	Malware Process
	72.21.91.29		15133	MCI Communications Services, Inc...	Malware Process
	23.35.171.27		20940	Akamai Technologies, Inc.	Malware Process
	52.57.145.87		16509	Amazon Technologies Inc.	Malware Process
	23.4.181.163		16625	Akamai Technologies, Inc.	Malware Process
	204.79.197.200		8068	Microsoft Corporation	Malware Process
	172.217.10.46		15169	Google LLC	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
usage.toolbar.conduit-services.com	80	POST	1.1	Mozilla/4.0 (compatible...	1	20.3807711601
Path: /ToolbarUsage.ashx **URI:** http://usage.toolbar.conduit-services.com/ToolbarUsage.ashx						
servicemap.conduit-services.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	21.1245851517
Path: /Toolbar/?ownerId=CT3045275 **URI:** http://servicemap.conduit-services.com/Toolbar/?ownerId=CT3045275						
bittorrentbar2.ourtoolbar.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	25.3655161858
Path: /SetupFinish **URI:** http://bittorrentbar2.ourtoolbar.com/SetupFinish						
bittorrentbar2.ourtoolbar.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	25.4664390087
Path: /SetupFinish/ **URI:** http://bittorrentbar2.ourtoolbar.com/SetupFinish/						
bittorrentbar2.ourtoolbar.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	25.6394231319
Path: /welcome/default.aspx **URI:** http://bittorrentbar2.ourtoolbar.com/welcome/default.aspx						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	26.0708401203
Path: /downloads/install-complete **URI:** http://www.bittorrent.com/downloads/install-complete						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	2	29.6890032291
Path: /stylesheets/frog/grid.css?1406221364 **URI:** http://www.bittorrent.com/stylesheets/frog/grid.css?1406221364						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	2	29.6989510059

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /stylesheets/animate-custom.css?1453258658 **URI:** http://www.bittorrent.com/stylesheets/animate-custom.css?1453258658						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	2	29.6992430687
Path: /scripts/site/jquery.smartbanner.js **URI:** http://www.bittorrent.com/scripts/site/jquery.smartbanner.js						
fonts.googleapis.com	80	GET	1.1	Mozilla/4.0 (compatible...	2	29.6995391846
Path: /css?family=Open+Sans:300italic,400italic,600,300,400,700&subset=latin,cyrillic,latin-ext **URI:** http://fonts.googleapis.com/css?family=Open+Sans:300italic,400italic,600,300,400,700&subset=latin,cyrillic,latin-ext						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	2	29.7046921253
Path: /stylesheets/jquery.smartbanner.css?1409068875 **URI:** http://www.bittorrent.com/stylesheets/jquery.smartbanner.css?1409068875						
netdna.bootstrapcdn.com	80	GET	1.1	Mozilla/4.0 (compatible...	2	29.7109282017
Path: /font-awesome/4.0.3/css/font-awesome.css **URI:** http://netdna.bootstrapcdn.com/font-awesome/4.0.3/css/font-awesome.css						
fast.fonts.net	80	GET	1.1	Mozilla/4.0 (compatible...	5	29.7111730576
Path: /cssapi/84df605e-600d-4cfa-a1a4-bd36ef0a22ad.css **URI:** http://fast.fonts.net/cssapi/84df605e-600d-4cfa-a1a4-bd36ef0a22ad.css						
ajax.googleapis.com	80	GET	1.1	Mozilla/4.0 (compatible...	2	29.7880580425
Path: /ajax/libs/jquery/1.11.1/jquery.min.js **URI:** http://ajax.googleapis.com/ajax/libs/jquery/1.11.1/jquery.min.js						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	30.004914999
Path: /stylesheets/frog/frog.css?1466697757 **URI:** http://www.bittorrent.com/stylesheets/frog/frog.css?1466697757						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	30.005120039
Path: /stylesheets/frog/panels.css?1520374749 **URI:** http://www.bittorrent.com/stylesheets/frog/panels.css?1520374749						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	30.0069591999
Path: /stylesheets/animate-custom.css?1409068875 **URI:** http://www.bittorrent.com/stylesheets/animate-custom.css?1409068875						
netdna.bootstrapcdn.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	30.5738611221
Path: /font-awesome/4.0.3/fonts/fontawesome-webfont.eot? **URI:** http://netdna.bootstrapcdn.com/font-awesome/4.0.3/fonts/fontawesome-webfont.eot?						
fonts.gstatic.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	30.6140620708
Path: /s/opensans/v15/mem8YaGs126MiZpBA-U1Uw.eot **URI:** http://fonts.gstatic.com/s/opensans/v15/mem8YaGs126MiZpBA-U1Uw.eot						
usage.toolbar.conduit-services.com	80	POST	1.1	Mozilla/4.0 (compatible...	1	31.5906190872
Path: /ToolbarUsage.ashx **URI:** http://usage.toolbar.conduit-services.com/ToolbarUsage.ashx						
www.googletagservices.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	32.4911360741
Path: /tag/js/gpt.js **URI:** http://www.googletagservices.com/tag/js/gpt.js						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	32.8031170368

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /scripts/site/detection.js **URI:** http://www.bittorrent.com/scripts/site/detection.js						
www.googleadservices.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	33.069272995
Path: /pagead/conversion.js **URI:** http://www.googleadservices.com/pagead/conversion.js						
settings.toolbar.search.conduit.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	33.4205992222
Path: /root/CT3045275/CT3045275 **URI:** http://settings.toolbar.search.conduit.com/root/CT3045275/CT3045275						
appsmetadata.toolbar.conduit-services.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	33.4229450226
Path: /?ctid=CT3045275 **URI:** http://appsmetadata.toolbar.conduit-services.com/?ctid=CT3045275						
clientlog.users.conduit.com	80	POST	1.1	Mozilla/4.0 (compatible...	1	33.5292751789
Path: / **URI:** http://clientlog.users.conduit.com/						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	51.0766351223
Path: /scripts/site/respond.min.js?1371775856 **URI:** http://www.bittorrent.com/scripts/site/respond.min.js?1371775856						
html5shiv.googlecode.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	51.0851671696
Path: /svn/trunk/html5.js **URI:** http://html5shiv.googlecode.com/svn/trunk/html5.js						
cdn.optimizely.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	51.1094050407
Path: /js/50136351.js **URI:** http://cdn.optimizely.com/js/50136351.js						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	52.5178902149
Path: /75/304/CT3045275/Images/634220815653506250.png **URI:** http://storage.stgbssint.com/75/304/CT3045275/Images/634220815653506250.png						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	52.6444151402
Path: /images/searchengines/go_btn_new.gif **URI:** http://storage.stgbssint.com/images/searchengines/go_btn_new.gif						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	52.7442290783
Path: /MarketPlace/93/ce3/93951332-f9a7-4af7-af02-17ec3d749ce3/Appearance/634159521796627506_24x24.png **URI:** http://storage.stgbssint.com/MarketPlace/93/ce3/93951332-f9a7-4af7-af02-17ec3d749ce3/Appearance/634159521796627506_24x24.png						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	52.7463200092
Path: /92/279/CT2790392/Images/634220879921318750.png **URI:** http://storage.stgbssint.com/92/279/CT2790392/Images/634220879921318750.png						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	52.8635940552
Path: /75/304/CT3045275/images/634818561434829991_24PX.png **URI:** http://storage.stgbssint.com/75/304/CT3045275/images/634818561434829991_24PX.png						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	53.0159420967
Path: /75/304/CT3045275/Images/634225281783662500.png **URI:** http://storage.stgbssint.com/75/304/CT3045275/Images/634225281783662500.png						

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	53.0215451717
Path: /92/279/CT2790392/Images/634225278165850000.png **URI:** http://storage.stgbssint.com/92/279/CT2790392/Images/634225278165850000.png						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	53.1359660625
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9523e74017f82604 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9523e74017f82604						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	53.4630131721
Path: /92/279/CT2790392/Images/634225280526593750.png **URI:** http://storage.stgbssint.com/92/279/CT2790392/Images/634225280526593750.png						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	53.4646670818
Path: /92/279/CT2790392/Images/634225279692725000.png **URI:** http://storage.stgbssint.com/92/279/CT2790392/Images/634225279692725000.png						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	53.628442049
Path: /92/279/CT2790392/Images/634225280304131250.png **URI:** http://storage.stgbssint.com/92/279/CT2790392/Images/634225280304131250.png						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	53.6287231445
Path: /92/279/CT2790392/Images/634225281436162500.png **URI:** http://storage.stgbssint.com/92/279/CT2790392/Images/634225281436162500.png						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	53.6312952042
Path: /92/279/CT2790392/Images/634225280643975000.png **URI:** http://storage.stgbssint.com/92/279/CT2790392/Images/634225280643975000.png						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	53.6315581799
Path: /92/279/CT2790392/Images/634225284383662500.png **URI:** http://storage.stgbssint.com/92/279/CT2790392/Images/634225284383662500.png						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	53.6319351196
Path: /92/279/CT2790392/Images/634225284881631250.png **URI:** http://storage.stgbssint.com/92/279/CT2790392/Images/634225284881631250.png						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	53.6320869923
Path: /92/279/CT2790392/Images/634225279948156250.png **URI:** http://storage.stgbssint.com/92/279/CT2790392/Images/634225279948156250.png						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	53.7918970585
Path: /92/279/CT2790392/Images/634225287181631250.png **URI:** http://storage.stgbssint.com/92/279/CT2790392/Images/634225287181631250.png						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	53.7929019928
Path: /92/279/CT2790392/Images/634225287547412500.png **URI:** http://storage.stgbssint.com/92/279/CT2790392/Images/634225287547412500.png						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	53.7939381599
Path: /75/304/CT3045275/Images/634244833256762500.png **URI:** http://storage.stgbssint.com/75/304/CT3045275/Images/634244833256762500.png						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	53.7949211597

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /75/304/CT3045275/Images/634226713903631250.png **URI:** http://storage.stgbssint.com/75/304/CT3045275/Images/634226713903631250.png						
contextmenu.toolbar.conduit-services.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	54.8006532192
Path: /?name=Toolbar&locale=EB_LOCALE&ctid=CT3045275&UM=UM_UNINSTALL_ID **URI:** http://contextmenu.toolbar.conduit-services.com/?name=Toolbar&locale=EB_LOCALE&ctid=CT3045275&UM=UM_UNINSTALL_ID						
contextmenu.toolbar.conduit-services.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	54.8009021282
Path: /?name=SharedApps&locale=EB_LOCALE&ctid=CT3045275 **URI:** http://contextmenu.toolbar.conduit-services.com/?name=SharedApps&locale=EB_LOCALE&ctid=CT3045275						
contextmenu.toolbar.conduit-services.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	54.8011381626
Path: /?name=OtherApps&locale=EB_LOCALE&ctid=CT3045275 **URI:** http://contextmenu.toolbar.conduit-services.com/?name=OtherApps&locale=EB_LOCALE&ctid=CT3045275						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	54.93404603
Path: /images/searchengines/search_icon.gif **URI:** http://storage.stgbssint.com/images/searchengines/search_icon.gif						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	54.9378581047
Path: /images/SearchEngines/images_search.gif **URI:** http://storage.stgbssint.com/images/SearchEngines/images_search.gif						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	54.941478014
Path: /images/SearchEngines/video.gif **URI:** http://storage.stgbssint.com/images/SearchEngines/video.gif						
contextmenu.toolbar.conduit-services.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.0191071033
Path: /?name=GottenApps&locale=EB_LOCALE&ctid=CT3045275 **URI:** http://contextmenu.toolbar.conduit-services.com/?name=GottenApps&locale=EB_LOCALE&ctid=CT3045275						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.0900981426
Path: /images/SearchEngines/news_icon.gif **URI:** http://storage.stgbssint.com/images/SearchEngines/news_icon.gif						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.0910441875
Path: /images/SearchEngines/tfd.gif **URI:** http://storage.stgbssint.com/images/SearchEngines/tfd.gif						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.0919551849
Path: /images/searchengines/softonic.gif **URI:** http://storage.stgbssint.com/images/searchengines/softonic.gif						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.0928590298
Path: /images/main_menu_upgrade.gif **URI:** http://storage.stgbssint.com/images/main_menu_upgrade.gif						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.0939362049
Path: /bankImages/ConduitEngine/ContextMenu/LikeIcon.png **URI:** http://storage.stgbssint.com/bankImages/ConduitEngine/ContextMenu/LikeIcon.png						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.0948710442
Path: /images/main_menu_help.gif **URI:** http://storage.stgbssint.com/images/main_menu_help.gif						

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	55.0999310017
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?97b9110e505395f1 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?97b9110e505395f1						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.2009680271
Path: /images/main_menu_privacy.gif **URI:** http://storage.stgbssint.com/images/main_menu_privacy.gif						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.2011442184
Path: /images/main_menu_home_page.gif **URI:** http://storage.stgbssint.com/images/main_menu_home_page.gif						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.2012500763
Path: /images/main_menu_about.gif **URI:** http://storage.stgbssint.com/images/main_menu_about.gif						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.2013921738
Path: /images/main_menu_contact.gif **URI:** http://storage.stgbssint.com/images/main_menu_contact.gif						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.2014930248
Path: /images/eula.png **URI:** http://storage.stgbssint.com/images/eula.png						
tbclient.tbccint.com	80	GET	1.1		1	55.3381581306
Path: /plugins/pricegong/Download/{5E1360DC-8FA8-40df-A8CD-FC3831B3634B}.cpi **URI:** http://tbclient.tbccint.com/plugins/pricegong/Download/{5E1360DC-8FA8-40df-A8CD-FC3831B3634B}.cpi						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.5978951454
Path: /images/main_menu_options.gif **URI:** http://storage.stgbssint.com/images/main_menu_options.gif						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.6065781116
Path: /images/main_menu_shrink.gif **URI:** http://storage.stgbssint.com/images/main_menu_shrink.gif						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.6069421768
Path: /images/main_menu_clear_history.gif **URI:** http://storage.stgbssint.com/images/main_menu_clear_history.gif						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.6072201729
Path: /images/main_menu_refresh.gif **URI:** http://storage.stgbssint.com/images/main_menu_refresh.gif						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	55.6205911636
Path: /images/Menu/uninstall-icon.png **URI:** http://storage.stgbssint.com/images/Menu/uninstall-icon.png						
emailnotifier.services.conduit.com	80	POST	1.1	Mozilla/4.0 (compatible...	1	56.4074790478
Path: /MailProvider/MailProvidersServices.asmx/GetMailProvidersInfo **URI:** http://emailnotifier.services.conduit.com/MailProvider/MailProvidersServices.asmx/GetMailProvidersInfo						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	56.7790951729
Path: /ps/searchmod/embedded.html **URI:** http://storage.stgbssint.com/ps/searchmod/embedded.html						

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
rss.cnn.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	56.810790062
Path: /rss/cnn_latest.rss **URI:** http://rss.cnn.com/rss/cnn_latest.rss						
toolbarstats.s3.amazonaws.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	56.8470630646
Path: /stats_dyn.html?tbv=1&tbn=0 **URI:** http://toolbarstats.s3.amazonaws.com/stats_dyn.html?tbv=1&tbn=0						
storage.Conduit.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	56.8932330608
Path: /bankImages/ConduitEngine/ContextMenu/More.png **URI:** http://storage.Conduit.com/bankImages/ConduitEngine/ContextMenu/More.png						
storage.Conduit.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	56.8975410461
Path: /bankImages/ConduitEngine/ContextMenu/LikeIcon.png **URI:** http://storage.Conduit.com/bankImages/ConduitEngine/ContextMenu/LikeIcon.png						
storage.Conduit.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	56.8977169991
Path: /bankImages/ConduitEngine/ContextMenu/Upgrade.png **URI:** http://storage.Conduit.com/bankImages/ConduitEngine/ContextMenu/Upgrade.png						
storage.Conduit.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	56.9015710354
Path: /bankImages/ConduitEngine/ContextMenu/Browse.png **URI:** http://storage.Conduit.com/bankImages/ConduitEngine/ContextMenu/Browse.png						
storage.Conduit.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	56.9017570019
Path: /bankImages/ConduitEngine/ContextMenu/Options.png **URI:** http://storage.Conduit.com/bankImages/ConduitEngine/ContextMenu/Options.png						
storage.Conduit.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	56.9019331932
Path: /bankImages/ConduitEngine/ContextMenu/Refresh.png **URI:** http://storage.Conduit.com/bankImages/ConduitEngine/ContextMenu/Refresh.png						
weather.tbccint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	56.9021902084
Path: /weatherrequest.ctp?type=search&platform=IE&source=1&ctid=CT3045275&octid=CT3045275&locale=en&cityname=ebifeellucky **URI:** http://weather.tbccint.com/weatherrequest.ctp?type=search&platform=IE&source=1&ctid=CT3045275&octid=CT3045275&locale=en&cityname=ebifeellucky						
storage.Conduit.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	56.9914970398
Path: /bankImages/ConduitEngine/ContextMenu/Hide.png **URI:** http://storage.Conduit.com/bankImages/ConduitEngine/ContextMenu/Hide.png						
storage.Conduit.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	57.0019261837
Path: /bankImages/ConduitEngine/ContextMenu/Privacy.png **URI:** http://storage.Conduit.com/bankImages/ConduitEngine/ContextMenu/Privacy.png						
storage.Conduit.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	57.0113081932
Path: /bankImages/ConduitEngine/ContextMenu/About.png **URI:** http://storage.Conduit.com/bankImages/ConduitEngine/ContextMenu/About.png						
storage.Conduit.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	57.0114891529
Path: /bankImages/ConduitEngine/ContextMenu/Contact.png **URI:** http://storage.Conduit.com/bankImages/ConduitEngine/ContextMenu/Contact.png						
storage.Conduit.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	57.0300111771

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /bankImages/ConduitEngine/ContextMenu/MoreFromPublisher.png **URI:** http://storage.Conduit.com/bankImages/ConduitEngine/ContextMenu/MoreFromPublisher.png						
users.conduit.com	80	POST	1.1	Mozilla/4.0 (compatible...	1	57.2974700928
Path: /iis2ebs.asp **URI:** http://users.conduit.com/iis2ebs.asp						
api.conduit.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	57.3989059925
Path: /BrowserCompApi.js **URI:** http://api.conduit.com/BrowserCompApi.js						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	57.6066770554
Path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?b1b146edf77dacad **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?b1b146edf77dacad						
login.toolbar.conduit-services.com	80	POST	1.1	Mozilla/4.0 (compatible...	1	57.6916282177
Path: /Login.ashx **URI:** http://login.toolbar.conduit-services.com/Login.ashx						
crl.geotrust.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	57.7218341827
Path: /crls/secureca.crl **URI:** http://crl.geotrust.com/crls/secureca.crl						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	57.9715850353
Path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?8ee644403b605cdb **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?8ee644403b605cdb						
g.symcd.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	58.2569210529
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSxtDkXkBa3l3lQEfFgudSiPNvt7gQUAPkqw0GRtsnCuD5V8sCXEROgByACEAEAISWIsPpZp3fvBXtmJ98%3D **URI:** http://g.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSxtDkXkBa3l3lQEfFgudSiPNvt7gQUAPkqw0GRtsnCuD5V8sCXEROgByACEAEAISWIsPpZp3fvBXtmJ98%3D						
newtab.conduit-hosting.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	58.5889070034
Path: /newtab/?ctid=CT3045275&UM=UM_ID **URI:** http://newtab.conduit-hosting.com/newtab/?ctid=CT3045275&UM=UM_ID						
ocsp.pki.goog	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	58.602268219
Path: /gsr2/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBTgXIsxbvr2lBkPpoIEVRE6gHlCnAQUm%2BIHV2ccHsBqBt5ZtJot39wZhi4CDQHjqTAc%2FHIGOD%2BaUx0%3D **URI:** http://ocsp.pki.goog/gsr2/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBTgXIsxbvr2lBkPpoIEVRE6gHlCnAQUm%2BIHV2ccHsBqBt5ZtJot39wZhi4CDQHjqTAc%2FHIGOD%2BaUx0%3D						
www.google-analytics.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	58.9654970169
Path: /ga.js **URI:** http://www.google-analytics.com/ga.js						
clients1.google.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	58.9856171608
Path: /ocsp/MEkwRzBFMEMwQTAJBgUrDgMCGgUABBTy4Gr5hYodjXCbSRkjeqm1Gih%2BZAQUSt0GFhu89mi1dvWBtrtiGrpagS8CCCl7eXoFMPpY **URI:** http://clients1.google.com/ocsp/MEkwRzBFMEMwQTAJBgUrDgMCGgUABBTy4Gr5hYodjXCbSRkjeqm1Gih%2BZAQUSt0GFhu89mi1dvWBtrtiGrpagS8CCCl7eXoFMPpY						
ocsp.pki.goog	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	59.3792951107
Path: /GTSGIAG3/MEkwRzBFMEMwQTAJBgUrDgMCGgUABBT27bBjYjKBmjX2jXWgnQJKEapsrQQUd8K4UJpndnaxLcKG0IOgfqZ%2BuksCCAqPCnhmlE7t **URI:** http://ocsp.pki.goog/GTSGIAG3/MEkwRzBFMEMwQTAJBgUrDgMCGgUABBT27bBjYjKBmjX2jXWgnQJKEapsrQQUd8K4UJpndnaxLcKG0IOgfqZ%2BuksCCAqPCnhmlE7t						

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
crl.pki.goog	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	59.4059841633
Path: /GTSGIAG3.crl **URI:** http://crl.pki.goog/GTSGIAG3.crl						
api.search.conduit.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	59.4416100979
Path: /Settings/?ctid=CT3045275&um=UM_ID **URI:** http://api.search.conduit.com/Settings/?ctid=CT3045275&um=UM_ID						
counting.usage.toolbar.conduit-services.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	62.7421290874
Path: /usage.ashx **URI:** http://counting.usage.toolbar.conduit-services.com/usage.ashx						
tracking.usage.app.conduit-services.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	63.0251231194
Path: /FirstTime.ashx?current=New **URI:** http://tracking.usage.app.conduit-services.com/FirstTime.ashx?current=New						
settings.pricegong.com	80	GET	1.1	Microsoft-ATL-Native/1...	2	63.0394070148
Path: /settings.ashx?bt=ie&bv=8.0.7601.17514&os=6.1_Service%20Pack%201&defbt=ff&pver=1&app=PriceGong&cver=3.6.12&pglv=&cnum=20503A4E-080027CB305F&unum=8B4736B7-0F0F-4CDB-AD72-8751D2A6FEBA&disid=cndt&subdisid=CT3045275&tbn=BitTorrentBar2&cdate=&ct=&ug=&cxt=2&impr=5&&ts=0&inst=0&snz=0&du=0&zs=1 **URI:** http://settings.pricegong.com/settings.ashx?bt=ie&bv=8.0.7601.17514&os=6.1_Service%20Pack%201&defbt=ff&pver=1&app=PriceGong&cver=3.6.12&pglv=&cnum=20503A4E-080027CB305F&unum=8B4736B7-0F0F-4CDB-AD72-8751D2A6FEBA&disid=cndt&subdisid=CT3045275&tbn=BitTorrentBar2&cdate=&ct=&ug=&cxt=2&impr=5&&ts=0&inst=0&snz=0&du=0&zs=1						
clientlog.users.tbccint.com	80	POST	1.1	Mozilla/4.0 (compatible...	1	63.5626590252
Path: /ClientDiagnostics.asmx/ReportDiagnosticsEvent **URI:** http://clientlog.users.tbccint.com/ClientDiagnostics.asmx/ReportDiagnosticsEvent						
b.scorecardresearch.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	66.4819672108
Path: /beacon.js **URI:** http://b.scorecardresearch.com/beacon.js						
static.bitmedianetwork.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	66.4824390411
Path: /ados.js **URI:** http://static.bitmedianetwork.com/ados.js						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	67.074311018
Path: /images/logo/logo.png **URI:** http://www.bittorrent.com/images/logo/logo.png						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	67.0746610165
Path: /images/logo/bt_pro.png **URI:** http://www.bittorrent.com/images/logo/bt_pro.png						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	67.1272540092
Path: /scripts/frog/b2.js?1469053878 **URI:** http://www.bittorrent.com/scripts/frog/b2.js?1469053878						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	67.1437551975
Path: /stylesheets/animate-custom.css?1453258658 **URI:** http://www.bittorrent.com/stylesheets/animate-custom.css?1453258658						

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	67.1440842152
Path: /images/site/ui_divider.gif **URI:** http://www.bittorrent.com/images/site/ui_divider.gif						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	67.144382
Path: /scripts/frog/vendor/jquery.vide.min.js? **URI:** http://www.bittorrent.com/scripts/frog/vendor/jquery.vide.min.js?						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	67.1656470299
Path: /scripts/site/retina-1.1.0.min.js **URI:** http://www.bittorrent.com/scripts/site/retina-1.1.0.min.js						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	67.1790971756
Path: /scripts/frog/frog.js?1488849741 **URI:** http://www.bittorrent.com/scripts/frog/frog.js?1488849741						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	67.3000741005
Path: /scripts/tracking.js **URI:** http://www.bittorrent.com/scripts/tracking.js						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	67.3511362076
Path: /images/logo/bt_now.png **URI:** http://www.bittorrent.com/images/logo/bt_now.png						
edge.quantserve.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	67.3554611206
Path: /quant.js **URI:** http://edge.quantserve.com/quant.js						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	67.3988420963
Path: /scripts/site/jquery.colorbox-min.js **URI:** http://www.bittorrent.com/scripts/site/jquery.colorbox-min.js						
engine.bitmedianetwork.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	67.7615170479
Path: /ados?t=1523632575922&request={"Placements":[{"A":5682,"S":50614,"D":"azk78385","ATA":[4,925],"Z":[57118],"Properties":{"x-index-domain":"bitmedianetwork.com"}}],"Keywords":"undefined","Referrer":"","IsAsync":true} **URI:** http://engine.bitmedianetwork.com/ados?t=1523632575922&request={"Placements":[{"A":5682,"S":50614,"D":"azk78385","ATA":[4,925],"Z":[57118],"Properties":{"x-index-domain":"bitmedianetwork.com"}}],"Keywords":"undefined","Referrer":"","IsAsync":true}						
b.scorecardresearch.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	67.857984066
Path: /b?c1=2&c2=17330952&ns__t=1523632575940&ns_c=windows-1252&ns_if=1&cv=3.1&c8=Download%20-%20BitTorrent%C2%AE%20-%20Delivering%20the%20World%E2%80%99s%20Content&c7=http%3A%2F%2Fwww.bittorrent.com%2Fdownloads%2Finstall-complete&c9= **URI:** http://b.scorecardresearch.com/b?c1=2&c2=17330952&ns__t=1523632575940&ns_c=windows-1252&ns_if=1&cv=3.1&c8=Download%20-%20BitTorrent%C2%AE%20-%20Delivering%20the%20World%E2%80%99s%20Content&c7=http%3A%2F%2Fwww.bittorrent.com%2Fdownloads%2Finstall-complete&c9=						
weather.tbccint.com	80	GET	1.1	Mozilla/4.0 (compatible...	3	68.8721241951
Path: /weatherrequest.ctp?type=forecast&imagetype=DEFAULT&ndays=3&locale=en&locationid=USNY0181 **URI:** http://weather.tbccint.com/weatherrequest.ctp?type=forecast&imagetype=DEFAULT&ndays=3&locale=en&locationid=USNY0181						
pixel.quantserve.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	68.9062671661

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /pixel;r=1197553828;rf=2;a=p-f87ZgUEkM-SZY;url=http%3A%2F%2Fwww.bittorrent.com%2Fdownloads%2Finstall-complete;fpan=1;fpa=P0-132630905-1523636720685;ns=0;ce=1;cm=;ref=;je=1;sr=800x600x32;enc=n;dst=1;et=1523636720667;tzo=-180;ogl=url.http%3A%2F%2Fwww%252Ebittorrent%252Ecom%2Fdownloads%2Finstall-complete%2Ctype.website%2Ctitle.Download%20-%20BitTorrent%C2%AE%20-%20Delivering%20the%20World%E2%80%99s%20Content%2Cdescription.Download%20the%20official%20BitTorrent%C2%AE%20torrent%20client%20for%20Windows%20or%20Mac%E2%80%94from%20the%20inv%2Cimage.http%3A%2F%2Fwww%252Ebittorrent%252Ecom%2Fimages%2Flogo%2Fbtlogo%252Ejpg **URI:** http://pixel.quantserve.com/pixel;r=1197553828;rf=2;a=p-f87ZgUEkM-SZY;url=http%3A%2F%2Fwww.bittorrent.com%2Fdownloads%2Finstall-complete;fpan=1;fpa=P0-132630905-1523636720685;ns=0;ce=1;cm=;ref=;je=1;sr=800x600x32;enc=n;dst=1;et=1523636720667;tzo=-180;ogl=url.http%3A%2F%2Fwww%252Ebittorrent%252Ecom%2Fdownloads%2Finstall-complete%2Ctype.website%2Ctitle.Download%20-%20BitTorrent%C2%AE%20-%20Delivering%20the%20World%E2%80%99s%20Content%2Cdescription.Download%20the%20official%20BitTorrent%C2%AE%20torrent%20client%20for%20Windows%20or%20Mac%E2%80%94from%20the%20inv%2Cimage.http%3A%2F%2Fwww%252Ebittorrent%252Ecom%2Fimages%2Flogo%2Fbtlogo%252Ejpg						
clientlog.users.tbccint.com	80	POST	1.1	Mozilla/4.0 (compatible...	1	68.9379601479
Path: /ClientDiagnostics.asmx/ReportDiagnosticsEvent **URI:** http://clientlog.users.tbccint.com/ClientDiagnostics.asmx/ReportDiagnosticsEvent						
www.google-analytics.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	70.0071630478
Path: /__utm.gif?utmwv=5.7.1&utms=1&utmn=52160543&utmhn=storage.stgbssint.com&utmt=event&utme=5(User_State*NU_After_Feb01)&utmcs=utf-8&utmsr=800x600&utmvp=1x26&utmsc=32-bit&utmul=en-us&utmje=1&utmfl=20.0%20r0&utmdt=Search%20App%20-%20Embedded&utmhid=951010623&utmr=-&utmp=%2Fps%2Fsearchmod%2Fembedded.html&utmht=1523641505354&utmac=UA-38050659-1&utmcc=__utma%3D1.604918213.1523620961.1523620961.1523620961.1%3B%2B__utmz%3D1.1523620961.1.1.utmcsr%3D(direct)%7Cutmccn%3D(direct)%7Cutmmd%3D(none)%3B&utmjid=&utmu=4BAAAAAAAAAAAAAAAAAAAAAE~ **URI:** http://www.google-analytics.com/__utm.gif?utmwv=5.7.1&utms=1&utmn=52160543&utmhn=storage.stgbssint.com&utmt=event&utme=5(User_State*NU_After_Feb01)&utmcs=utf-8&utmsr=800x600&utmvp=1x26&utmsc=32-bit&utmul=en-us&utmje=1&utmfl=20.0%20r0&utmdt=Search%20App%20-%20Embedded&utmhid=951010623&utmr=-&utmp=%2Fps%2Fsearchmod%2Fembedded.html&utmht=1523641505354&utmac=UA-38050659-1&utmcc=__utma%3D1.604918213.1523620961.1523620961.1523620961.1%3B%2B__utmz%3D1.1523620961.1.1.utmcsr%3D(direct)%7Cutmccn%3D(direct)%7Cutmmd%3D(none)%3B&utmjid=&utmu=4BAAAAAAAAAAAAAAAAAAAAAE~						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	70.5552790165
Path: /stylesheets/frog/frog.css?1466697757 **URI:** http://www.bittorrent.com/stylesheets/frog/frog.css?1466697757						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	71.5647461414
Path: /stylesheets/frog/panels.css?1520374749 **URI:** http://www.bittorrent.com/stylesheets/frog/panels.css?1520374749						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	71.5651710033
Path: /faviconNew.ico **URI:** http://www.bittorrent.com/faviconNew.ico						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	71.6684501171
Path: /images/colorbox/cancel.png **URI:** http://www.bittorrent.com/images/colorbox/cancel.png						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	71.8777601719
Path: /stylesheets/jquery.smartbanner.css?1409068875 **URI:** http://www.bittorrent.com/stylesheets/jquery.smartbanner.css?1409068875						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	72.493817091
Path: /stylesheets/frog/grid.css?1406221364 **URI:** http://www.bittorrent.com/stylesheets/frog/grid.css?1406221364						
toolbarstats.s3.amazonaws.com	80	GET	1.1	Mozilla/4.0 (compatible...	2	72.5318391323
Path: /stats_dyn.html?tbv=1&tbn=0 **URI:** http://toolbarstats.s3.amazonaws.com/stats_dyn.html?tbv=1&tbn=0						
rss.cnn.com	80	GET	1.1	Mozilla/4.0 (compatible...	2	72.5397191048

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /rss/cnn_latest.rss **URI:** http://rss.cnn.com/rss/cnn_latest.rss						
feeds.reuters.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	72.5719151497
Path: /reuters/topNews **URI:** http://feeds.reuters.com/reuters/topNews						
rss.news.yahoo.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	72.7822601795
Path: /rss/world **URI:** http://rss.news.yahoo.com/rss/world						
news.google.nl	80	GET	1.1	Mozilla/4.0 (compatible...	1	72.7923910618
Path: /news?pz=1&cf=all&ned=nl_nl&hl=nl&topic=h&num=3&output=rss **URI:** http://news.google.nl/news?pz=1&cf=all&ned=nl_nl&hl=nl&topic=h&num=3&output=rss						
news.google.nl	80	GET	1.1	Mozilla/4.0 (compatible...	1	72.7955551147
Path: /news?cf=all&ned=us&hl=en&topic=h&num=3&output=rss **URI:** http://news.google.nl/news?cf=all&ned=us&hl=en&topic=h&num=3&output=rss						
feeds.news.com.au	80	GET	1.1	Mozilla/4.0 (compatible...	2	72.8021240234
Path: /public/rss/2.0/news_breaking_news_32.xml **URI:** http://feeds.news.com.au/public/rss/2.0/news_breaking_news_32.xml						
rss.cbc.ca	80	GET	1.1	Mozilla/4.0 (compatible...	1	72.8057091236
Path: /lineup/latest.xml **URI:** http://rss.cbc.ca/lineup/latest.xml						
newsrss.bbc.co.uk	80	GET	1.1	Mozilla/4.0 (compatible...	1	72.8089771271
Path: /rss/newsonline_world_edition/front_page/rss.xml **URI:** http://newsrss.bbc.co.uk/rss/newsonline_world_edition/front_page/rss.xml						
www.thesun.co.uk	80	GET	1.1	Mozilla/4.0 (compatible...	2	72.8222970963
Path: /sol/homepage/feeds/rss/article312900.ece **URI:** http://www.thesun.co.uk/sol/homepage/feeds/rss/article312900.ece						
worldpress.org	80	GET	1.1	Mozilla/4.0 (compatible...	1	72.8313760757
Path: /feeds/topstories.xml **URI:** http://worldpress.org/feeds/topstories.xml						
www.google-analytics.com	80	GET	1.1	Mozilla/4.0 (compatible...	2	72.9932320118
Path: /ga.js **URI:** http://www.google-analytics.com/ga.js						
news.google.nl	80	GET	1.1	Mozilla/4.0 (compatible...	1	73.0466601849
Path: /news/headlines **URI:** http://news.google.nl/news/headlines						
news.google.nl	80	GET	1.1	Mozilla/4.0 (compatible...	1	73.0485510826
Path: /news/headlines **URI:** http://news.google.nl/news/headlines						
news.google.nl	80	GET	1.1	Mozilla/4.0 (compatible...	1	73.2710211277
Path: /news?cf=all&ned=fr&hl=fr&topic=h&num=3&output=rss **URI:** http://news.google.nl/news?cf=all&ned=fr&hl=fr&topic=h&num=3&output=rss						
www.bittorrent.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	73.3150122166

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /stylesheets/animate-custom.css?1409068875 **URI:** http://www.bittorrent.com/stylesheets/animate-custom.css?1409068875						
news.yahoo.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	73.6374790668
Path: /rss/world **URI:** http://news.yahoo.com/rss/world						
feeds.feedburner.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	73.6534581184
Path: /newscomaubreakingndm **URI:** http://feeds.feedburner.com/newscomaubreakingndm						
feeds.bbci.co.uk	80	GET	1.1	Mozilla/4.0 (compatible...	1	73.6536941528
Path: /news/rss.xml?edition=int **URI:** http://feeds.bbci.co.uk/news/rss.xml?edition=int						
www.cbc.ca	80	GET	1.1	Mozilla/4.0 (compatible...	1	73.6550531387
Path: /cmlink/rss-latest **URI:** http://www.cbc.ca/cmlink/rss-latest						
news.google.nl	80	GET	1.1	Mozilla/4.0 (compatible...	1	73.8274950981
Path: /news/headlines **URI:** http://news.google.nl/news/headlines						
clients1.google.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	2	74.4150512218
Path: /ocsp/MEkwRzBFMEMwQTAJBgUrDgMCGgUABBTy4Gr5hYodjXCbSRkjeqm1Gih%2BZAQUSt0GFhu89mi1dvWBtrtiGrpagS8CCDdf%2FhHl4xa%2B **URI:** http://clients1.google.com/ocsp/MEkwRzBFMEMwQTAJBgUrDgMCGgUABBTy4Gr5hYodjXCbSRkjeqm1Gih%2BZAQUSt0GFhu89mi1dvWBtrtiGrpagS8CCDdf%2FhHl4xa%2B						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	74.4344921112
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCzkdAQpVYowQUsT7DaQP4v0cB1JgmGggC72NkK8MCEATh56TcXPLzbcArQrhdFZ8%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCzkdAQpVYowQUsT7DaQP4v0cB1JgmGggC72NkK8MCEATh56TcXPLzbcArQrhdFZ8%3D						
ieupdate.tbccint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	77.4076070786
Path: /ver6.18.2.72/tbedrs.dll **URI:** http://ieupdate.tbccint.com/ver6.18.2.72/tbedrs.dll						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	89.3972220421
Path: /pki/crl/products/tspca.crl **URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	89.5908172131
Path: /pki/crl/products/CodeSignPCA2.crl **URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	89.6378521919
Path: /pki/crl/products/WinPCA.crl **URI:** http://crl.microsoft.com/pki/crl/products/WinPCA.crl						
crl.globalsign.net	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	90.1349041462
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						
servicemap.tbccint.com	80	GET	1.1	Mozilla/4.0 (compatible...	2	91.2408590317

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /Toolbarservice **URI:** http://servicemap.tbccint.com/Toolbarservice						
search.conduit.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	96.2055752277
Path: /favicon.ico **URI:** http://search.conduit.com/favicon.ico						
usage.toolbar.tbccint.com	80	POST	1.1	Mozilla/4.0 (compatible...	3	104.852214098
Path: /ToolbarUsage.ashx **URI:** http://usage.toolbar.tbccint.com/ToolbarUsage.ashx						
toolbar-ie-updater.tbccint.com	80	GET	1.1	Mozilla/4.0 (compatible...	2	105.471423149
Path: /update/?productId=TBUpdaterLogic&ver=0.0.0.0&itemId=7b13ec3e-999a-4b70-b9cb-2617b8323822 **URI:** http://toolbar-ie-updater.tbccint.com/update/?productId=TBUpdaterLogic&ver=0.0.0.0&itemId=7b13ec3e-999a-4b70-b9cb-2617b8323822						
settings.toolbar.search.conduit.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	123.3216362
Path: /root/CT3045275/CT3045275 **URI:** http://settings.toolbar.search.conduit.com/root/CT3045275/CT3045275						
login.toolbar.conduit-services.com	80	POST	1.1	Mozilla/4.0 (compatible...	1	123.357743025
Path: /Login.ashx **URI:** http://login.toolbar.conduit-services.com/Login.ashx						
appsmetadata.toolbar.conduit-services.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	123.948339224
Path: /?ctid=CT3045275 **URI:** http://appsmetadata.toolbar.conduit-services.com/?ctid=CT3045275						
contextmenu.toolbar.conduit-services.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	124.828441143
Path: /?name=Toolbar&locale=en&ctid=CT3045275&UM=UM_UNINSTALL_ID **URI:** http://contextmenu.toolbar.conduit-services.com/?name=Toolbar&locale=en&ctid=CT3045275&UM=UM_UNINSTALL_ID						
contextmenu.toolbar.conduit-services.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	124.828677177
Path: /?name=SharedApps&locale=en&ctid=CT3045275 **URI:** http://contextmenu.toolbar.conduit-services.com/?name=SharedApps&locale=en&ctid=CT3045275						
contextmenu.toolbar.conduit-services.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	124.82885313
Path: /?name=OtherApps&locale=en&ctid=CT3045275 **URI:** http://contextmenu.toolbar.conduit-services.com/?name=OtherApps&locale=en&ctid=CT3045275						
contextmenu.toolbar.conduit-services.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	124.945226192
Path: /?name=GottenApps&locale=en&ctid=CT3045275 **URI:** http://contextmenu.toolbar.conduit-services.com/?name=GottenApps&locale=en&ctid=CT3045275						
feeds.reuters.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	142.525673151
Path: /reuters/topNews **URI:** http://feeds.reuters.com/reuters/topNews						
worldpress.org	80	GET	1.1	Mozilla/4.0 (compatible...	1	142.529878139
Path: /feeds/topstories.xml **URI:** http://worldpress.org/feeds/topstories.xml						
rss.cbc.ca	80	GET	1.1	Mozilla/4.0 (compatible...	1	152.582033157
Path: /lineup/latest.xml **URI:** http://rss.cbc.ca/lineup/latest.xml						
feeds.feedburner.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	152.59475112

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /newscomaubreakingndm **URI:** http://feeds.feedburner.com/newscomaubreakingndm						
www.cbc.ca	80	GET	1.1	Mozilla/4.0 (compatible...	1	152.933142185
Path: /cmlink/rss-latest **URI:** http://www.cbc.ca/cmlink/rss-latest						
tb-service.databssint.com	80	POST	1.1	Mozilla/4.0 (compatible...	1	185.224830151
Path: / **URI:** http://tb-service.databssint.com/						
tb-service.databssint.com	80	POST	1.1	Mozilla/4.0 (compatible...	1	185.565253019
Path: / **URI:** http://tb-service.databssint.com/						
usage.toolbar.tbccint.com	80	POST	1.1	Mozilla/4.0 (compatible...	1	185.976245165
Path: /ToolbarUsage.ashx **URI:** http://usage.toolbar.tbccint.com/ToolbarUsage.ashx						
usage.toolbar.tbccint.com	80	POST	1.1	Mozilla/4.0 (compatible...	1	186.396472216
Path: /ToolbarUsage.ashx **URI:** http://usage.toolbar.tbccint.com/ToolbarUsage.ashx						
www.msftncsi.com	80	GET	1.1	Microsoft NCSI	1	186.496842146
Path: /ncsi.txt **URI:** http://www.msftncsi.com/ncsi.txt						
storage.stgbssint.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	187.253320217
Path: /IEBackgroundContainer/TBUpdaterLogic/4.0.0.2/TBUpdaterLogic.dll **URI:** http://storage.stgbssint.com/IEBackgroundContainer/TBUpdaterLogic/4.0.0.2/TBUpdaterLogic.dll						
www.bing.com	80	GET	1.1	Mozilla/4.0 (compatible...	1	188.972701073
Path: /favicon.ico **URI:** http://www.bing.com/favicon.ico						

DNS QUERIES

Request	Type
usage.toolbar.conduit-services.com	A
Answers - origin-toolbarusage.conduit-services.com (CNAME) - usage.toolbar.ams.conduit-services.com (CNAME) - 195.78.120.83 (A)	
servicemap.conduit-services.com	A
Answers - 195.78.120.80 (A) - servicemap.ams.conduit-services.com (CNAME) - origin-servicemap.conduit-services.com (CNAME)	
bittorrentbar2.ourtoolbar.com	A

Request	Type
Answers - 195.78.120.93 (A) - ams.ourtoolbar.com (CNAME)	
www.bittorrent.com	A
Answers - 69.28.187.228 (A) - bittorrent-1.hs.llnwd.net (CNAME)	
fonts.googleapis.com	A
Answers - googleadapis.l.google.com (CNAME) - 172.217.10.234 (A)	
netdna.bootstrapcdn.com	A
Answers - 205.185.216.42 (A) - cds.j3z9t3p6.hwcdn.net (CNAME) - 205.185.216.10 (A)	
fast.fonts.net	A
Answers - 93.184.216.182 (A) - fast.wac.1AC1.iotacdn.net (CNAME) - s9.gp1.wac.gammacdn.net (CNAME)	
ajax.googleapis.com	A
Answers - 172.217.12.170 (A) - 172.217.11.10 (A) - googleapis.l.google.com (CNAME) - 172.217.10.42 (A) - 172.217.12.202 (A) - 172.217.11.42 (A) - 172.217.3.106 (A) - 172.217.7.10 (A) - 216.58.219.234 (A) - 216.58.219.202 (A) - 172.217.6.234 (A)	
www.googleadservices.com	A
Answers - pagead.l.doubleclick.net (CNAME) - 172.217.6.226 (A)	
cdn.optimizely.com	A
Answers - 104.107.44.23 (A)	
html5shiv.googlecode.com	A
Answers - 173.194.68.82 (A) - googlecode.l.googleusercontent.com (CNAME)	
fonts.gstatic.com	A
Answers - 172.217.10.67 (A) - gstaticadssl.l.google.com (CNAME)	

Request	Type
www.googletagservices.com	A
Answers - pagead46.l.doubleclick.net (CNAME) - 172.217.12.194 (A)	
securepubads.g.doubleclick.net	A
Answers - partnerad.l.doubleclick.net (CNAME) - 172.217.10.226 (A)	
adservice.google.com	A
Answers - 172.217.10.66 (A)	
dynamicdialogs.toolbar.conduit-services.com	A
Answers - (NXDOMAIN)	
appsmetadata.toolbar.conduit-services.com	A
Answers - appsmetadata.toolbar.conduit-services.com.edgesuite.net (CNAME) - a1982.g1.akamai.net (CNAME) - 23.67.250.107 (A) - 23.67.250.112 (A)	
settings.toolbar.search.conduit.com	A
Answers - 23.67.250.115 (A) - a948.g1.akamai.net (CNAME) - settings.toolbar.conduit-services.com.edgesuite.net (CNAME) - 23.67.250.96 (A)	
clientlog.users.conduit.com	A
Answers - 195.78.120.79 (A) - clientlog.users.ams.conduit.com (CNAME) - origin-clienterrorlog.conduit.com (CNAME)	
storage.stgbssint.com	A
Answers - origin-storage.stgbssint.com (CNAME) - 195.78.120.65 (A) - storage.ams.stgbssint.com (CNAME)	
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 184.26.44.97 (A) - a1621.g.akamai.net (CNAME) - ctldl.windowsupdate.com.edgesuite.net (CNAME) - 184.26.44.105 (A)	
contextmenu.toolbar.conduit-services.com	A

Request	Type
Answers - a1742.g1.akamai.net (CNAME) - 23.67.250.120 (A) - contextmenu.toolbar.conduit-services.com.edgesuite.net (CNAME) - 23.67.250.138 (A)	
tbclient.tbccint.com	A
Answers - e6399.e8.akamaiedge.net (CNAME) - 23.200.109.88 (A) - tbccint.com.edgekey.net (CNAME)	
emailnotifier.services.conduit.com	A
Answers - emailnotifier.services.ams.conduit.com (CNAME) - origin-emailnotifierservices.conduit.com (CNAME) - 195.78.120.73 (A)	
cap1.conduit-apps.com	A
app.mam.vaccint.com	A
Answers - origin-app.mam.vaccint.com (CNAME) - 199.101.114.130 (A) - app.mam.va.vaccint.com (CNAME)	
rss.cnn.com	A
Answers - i0bub0.feedproxy.ghs.google.com (CNAME) - 172.217.10.51 (A)	
storage.conduit.com	A
Answers - storage.ams.conduit.com (CNAME)	
toolbarstats.s3.amazonaws.com	A
Answers - s3-1-w.amazonaws.com (CNAME) - 54.231.49.234 (A) - s3-directional-w.amazonaws.com (CNAME) - 52.216.229.99 (A) - 52.216.86.35 (A)	
weather.tbccint.com	A
Answers - 72.246.43.51 (A) - a1254.f.akamai.net (CNAME) - 72.246.43.9 (A) - tbccint.com.edgesuite.net (CNAME)	
login.toolbar.conduit-services.com	A
Answers - login.toolbar.ams.conduit-services.com (CNAME) - origin-toolbarlogin.conduit-services.com (CNAME) - 195.78.120.102 (A)	
users.conduit.com	A

Request	Type
Answers - 199.101.115.202 (A)	
api.conduit.com	A
Answers - origin-api.conduit.com (CNAME) - api.ams.conduit.com (CNAME) - 195.78.120.104 (A)	
crl.geotrust.com	A
Answers - 23.4.181.163 (A) - e6845.dscb1.akamaiedge.net (CNAME) - crl-ds.ws.symantec.com.edgekey.net (CNAME)	
g.symcd.com	A
Answers - ocsp-ds.ws.symantec.com.edgekey.net (CNAME) - e8218.dscb1.akamaiedge.net (CNAME) - 23.4.187.27 (A)	
newtab.conduit-hosting.com	A
Answers - newtab.conduit-hosting.com.edgesuite.net (CNAME) - 23.67.250.128 (A) - 23.67.250.121 (A) - a908.g1.akamai.net (CNAME)	
ocsp.pki.goog	A
Answers - 172.217.10.238 (A) - www3.l.google.com (CNAME)	
www.google-analytics.com	A
Answers - www-google-analytics.l.google.com (CNAME) - 172.217.6.238 (A)	
clients1.google.com	A
Answers - 172.217.3.110 (A) - clients.l.google.com (CNAME)	
crl.pki.goog	A
Answers - 172.217.10.46 (A)	
api.search.conduit.com	A
Answers - 199.101.114.106 (A) - origin-api.seccint.com (CNAME) - origin-searchapi.conduit.com (CNAME) - api.va.seccint.com (CNAME)	
counting.usage.toolbar.conduit-services.com	A
Answers - 199.101.114.251 (A)	

Request	Type
tracking.usage.app.conduit-services.com	A
Answers - 199.101.114.100 (A)	
settings.pricegong.com	A
Answers - 82.163.248.194 (A)	
clientlog.users.tbccint.com	A
Answers - origin-clientlog.users.tbccint.com (CNAME) - clientlog.users.ams.tbccint.com (CNAME)	
timeservice.conduit-services.com	A
Answers - origin-timeservice.conduit-services.com (CNAME) - timeservice.ams.conduit-services.com (CNAME) - 195.78.120.182 (A)	
b.scorecardresearch.com	A
Answers - a1294.w20.akamai.net (CNAME) - b.scorecardresearch.com.edgesuite.net (CNAME) - 184.26.44.104 (A)	
static.bitmedianetwork.com	A
Answers - 104.17.31.15 (A) - 104.17.29.15 (A) - static.adzerk.net (CNAME) - 104.17.28.15 (A) - 104.17.27.15 (A) - static.adzerk.net.cdn.cloudflare.net (CNAME) - 104.17.30.15 (A)	
edge.quantserve.com	A
Answers - 66.150.118.49 (A) - 66.150.118.61 (A) - 66.150.118.22 (A) - px-wdc102.quantserve.com.akadns.net (CNAME) - 66.150.118.35 (A) - 66.150.118.18 (A) - 66.150.118.26 (A) - 66.150.118.57 (A) - akamai-edge.quantserve.com.akadns.net (CNAME) - 66.150.118.16 (A)	
engine.bitmedianetwork.com	A
Answers - 54.243.137.87 (A) - 54.197.232.195 (A) - 23.23.236.103 (A) - bittorrent-954311581.us-east-1.elb.amazonaws.com (CNAME) - 54.225.184.50 (A) - 50.19.235.64 (A) - 54.243.33.238 (A)	

Request	Type
rules.quantcount.com	A
Answers - 52.85.101.89 (A) - 52.85.101.112 (A) - d2fashanjl7d9f.cloudfront.net (CNAME) - 52.85.101.145 (A) - 52.85.101.115 (A) - 52.85.101.218 (A) - 52.85.101.234 (A) - 52.85.101.20 (A) - 52.85.101.76 (A)	
ssum.casalemedia.com	A
Answers - 23.50.230.12 (A) - e8037.g.akamaiedge.net (CNAME) - ssum.casalemedia.com.edgekey.net (CNAME)	
pixel.quantserve.com	A
Answers - pixel-use201-lighttpd.pixel.quantserve.net (CNAME) - 18.216.230.190 (A) - 18.216.249.250 (A) - 18.216.66.161 (A) - 18.217.127.164 (A) - 18.217.188.215 (A) - 18.216.93.150 (A) - pixel-use201-lighttpd-elb-1612913623.us-east-2.elb.amazonaws.com (CNAME) - global.px.quantserve.com (CNAME) - 18.216.19.225 (A) - 18.216.121.156 (A)	
weather.conduit.com	A
s3.amazonaws.com	A
Answers - 52.216.101.21 (A) - s3-1.amazonaws.com (CNAME)	
feeds.reuters.com	A
Answers - reuters.feedproxy.ghs.google.com (CNAME)	
worldpress.org	A
Answers - 66.135.34.17 (A)	
rss.news.yahoo.com	A
Answers - media-router-rc1.prod.media.yahoo.com (CNAME) - 98.136.96.140 (A) - oob-media-router-rc1.prod.media.wg1.b.yahoo.com (CNAME) - 74.6.144.137 (A)	
news.google.nl	A
Answers - 172.217.10.35 (A) - news-cctld.l.google.com (CNAME)	

Request	Type
rss.cbc.ca	A
Answers - san.cbc.ca.edgekey.net (CNAME) - e5220.g.akamaiedge.net (CNAME) - 23.50.229.108 (A)	
newsrss.bbc.co.uk	A
Answers - newsrss.bbc.net.uk (CNAME) - 184.26.44.95 (A) - news.bbc.co.uk.edgesuite.net (CNAME) - a1733.g.akamai.net (CNAME)	
www.thesun.co.uk	A
Answers - 173.222.184.25 (A) - www.thesun.co.uk.edgekey.net (CNAME) - e3951.e12.akamaiedge.net (CNAME) - 104.106.251.24 (A)	
feeds.news.com.au	A
Answers - a964.g.akamai.net (CNAME) - 184.26.44.106 (A) - feeds.news.com.au.edgesuite.net (CNAME)	
feeds.bbci.co.uk	A
Answers - feeds.bbci.co.uk.edgekey.net (CNAME) - e3891.f.akamaiedge.net (CNAME) - 104.107.50.14 (A)	
www.cbc.ca	A
news.yahoo.com	A
feeds.feedburner.com	A
Answers - www4.l.google.com (CNAME)	
www.yahoo.com	A
Answers - 72.30.35.9 (A) - 98.138.219.231 (A) - 72.30.35.10 (A) - 98.138.219.232 (A) - atsv2-fp.wg1.b.yahoo.com (CNAME)	
news.google.com	A
Answers - news.l.google.com (CNAME)	
ocsp.digicert.com	A
Answers - cs9.wac.phicdn.net (CNAME) - 72.21.91.29 (A)	
ieupdate.tbccint.com	A

Request	Type
crl.microsoft.com	A
Answers - 184.26.44.98 (A) - crl.www.ms.akadns.net (CNAME) - a1363.dscg.akamai.net (CNAME)	
crl.globalsign.net	A
Answers - 104.31.75.124 (A) - global.prd.cdn.globalsign.com (CNAME) - cdn.globalsigncdn.com.cdn.cloudflare.net (CNAME) - 104.31.74.124 (A)	
servicemap.tbccint.com	A
Answers - servicemap.ams.tbccint.com (CNAME) - origin-servicemap.tbccint.com (CNAME)	
search.conduit.com	A
Answers - aws.trovi.com (CNAME) - se-p-search-app.us-east-1.elasticbeanstalk.com (CNAME) - 52.202.76.88 (A) - origin-www.aws.searchfuel.co (CNAME) - 34.198.95.87 (A)	
usage.toolbar.tbccint.com	A
Answers - usage.toolbar.ams.tbccint.com (CNAME) - origin-usage.toolbar.tbccint.com (CNAME)	
toolbar-ie-updater.tbccint.com	A
tb-service.databssint.com	A
Answers - 54.235.180.144 (A) - Jazz-1846647836.us-east-1.elb.amazonaws.com (CNAME) - 50.19.241.43 (A)	
www.msftncsi.com	A
Answers - www.msftncsi.com.edgesuite.net (CNAME) - 23.67.250.139 (A) - a1961.g2.akamai.net (CNAME)	
www.bing.com	A
Answers - www-bing-com.a-0001.a-msedge.net (CNAME) - 204.79.197.200 (A) - a-0001.a-msedge.net (CNAME) - 13.107.21.200 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
20.3807711601	Sandbox	195.78.120.83	80
21.1245851517	Sandbox	195.78.120.80	80
25.3655161858	Sandbox	195.78.120.93	80
26.0708401203	Sandbox	69.28.187.228	80
29.6890032291	Sandbox	69.28.187.228	80
29.6989510059	Sandbox	69.28.187.228	80
29.6992430687	Sandbox	69.28.187.228	80
29.6995391846	Sandbox	172.217.10.234	80
29.7046921253	Sandbox	69.28.187.228	80
29.7109282017	Sandbox	205.185.216.10	80
29.7111730576	Sandbox	93.184.216.182	80
29.7880580425	Sandbox	172.217.12.202	80
29.9978630543	Sandbox	205.185.216.10	80
29.9991970062	Sandbox	172.217.10.234	80
30.0024631023	Sandbox	69.28.187.228	80
30.0046761036	Sandbox	69.28.187.228	80
30.004914999	Sandbox	69.28.187.228	80
30.005120039	Sandbox	69.28.187.228	80
30.0067241192	Sandbox	69.28.187.228	80
30.0069591999	Sandbox	69.28.187.228	80
30.6140620708	Sandbox	172.217.10.67	80
31.2830941677	Sandbox	93.184.216.182	80
31.2855331898	Sandbox	93.184.216.182	80
31.5906190872	Sandbox	195.78.120.83	80
32.4887061119	Sandbox	172.217.12.202	80
32.4911360741	Sandbox	172.217.12.194	80
32.8031170368	Sandbox	69.28.187.228	80
32.9575581551	Sandbox	69.28.187.228	80
33.0265591145	Sandbox	172.217.10.226	443
33.069272995	Sandbox	172.217.6.226	80
33.0932161808	Sandbox	172.217.10.66	443
33.4205992222	Sandbox	23.67.250.115	80
33.4229450226	Sandbox	23.67.250.112	80
33.5292751789	Sandbox	195.78.120.79	80
51.0700411797	Sandbox	93.184.216.182	80
51.0703279972	Sandbox	93.184.216.182	80
51.0766351223	Sandbox	69.28.187.228	80

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
51.0851671696	Sandbox	173.194.68.82	80
51.1094050407	Sandbox	104.107.44.23	80
51.8292770386	Sandbox	172.217.10.226	443
51.8296880722	Sandbox	172.217.10.66	443
52.5178902149	Sandbox	195.78.120.65	80
52.7442290783	Sandbox	195.78.120.65	80
53.1359660625	Sandbox	184.26.44.97	80
53.628442049	Sandbox	195.78.120.65	80
53.6287231445	Sandbox	195.78.120.65	80
53.6312952042	Sandbox	195.78.120.65	80
53.6315581799	Sandbox	195.78.120.65	80
54.8006532192	Sandbox	23.67.250.138	80
54.8009021282	Sandbox	23.67.250.138	80
54.8011381626	Sandbox	23.67.250.138	80
55.3381581306	Sandbox	23.200.109.88	80
56.4074790478	Sandbox	195.78.120.73	80
56.810790062	Sandbox	172.217.10.51	80
56.8470630646	Sandbox	54.231.49.234	80
56.8932330608	Sandbox	195.78.120.65	80
56.8975410461	Sandbox	195.78.120.65	80
56.8977169991	Sandbox	195.78.120.65	80
56.9015710354	Sandbox	195.78.120.65	80
56.9017570019	Sandbox	195.78.120.65	80
56.9019331932	Sandbox	195.78.120.65	80
56.9021902084	Sandbox	72.246.43.51	80
57.2974700928	Sandbox	199.101.115.202	80
57.3989059925	Sandbox	195.78.120.104	80
57.6066770554	Sandbox	184.26.44.97	80
57.6916282177	Sandbox	195.78.120.102	80
57.7218341827	Sandbox	23.4.181.163	80
58.2569210529	Sandbox	23.4.187.27	80
58.5889070034	Sandbox	23.67.250.121	80
58.602268219	Sandbox	172.217.10.238	80
58.9654970169	Sandbox	172.217.6.238	80
58.9856171608	Sandbox	172.217.3.110	80
59.3792951107	Sandbox	172.217.10.238	80
59.4059841633	Sandbox	172.217.10.46	80

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
59.4416100979	Sandbox	199.101.114.106	80
62.7421290874	Sandbox	199.101.114.251	80
63.0251231194	Sandbox	199.101.114.100	80
63.0394070148	Sandbox	82.163.248.194	80
63.0766720772	Sandbox	82.163.248.194	443
63.5626590252	Sandbox	195.78.120.79	80
63.934607029	Sandbox	172.217.10.226	443
66.4819672108	Sandbox	184.26.44.104	80
66.4824390411	Sandbox	104.17.28.15	80
67.074311018	Sandbox	69.28.187.228	80
67.0746610165	Sandbox	69.28.187.228	80
67.1272540092	Sandbox	69.28.187.228	80
67.1440842152	Sandbox	69.28.187.228	80
67.144382	Sandbox	69.28.187.228	80
67.3554611206	Sandbox	66.150.118.61	80
67.7615170479	Sandbox	54.243.137.87	80
67.857984066	Sandbox	184.26.44.104	80
68.8721241951	Sandbox	72.246.43.51	80
68.9062671661	Sandbox	18.216.93.150	80
68.9379601479	Sandbox	195.78.120.79	80
70.0071630478	Sandbox	172.217.6.238	80
70.5552790165	Sandbox	69.28.187.228	80
71.5647461414	Sandbox	69.28.187.228	80
71.5651710033	Sandbox	69.28.187.228	80
72.0068440437	Sandbox	72.246.43.51	80
72.493817091	Sandbox	69.28.187.228	80
72.5318391323	Sandbox	52.216.229.99	80
72.5397191048	Sandbox	172.217.10.51	80
72.5719151497	Sandbox	172.217.10.51	80
72.7822601795	Sandbox	74.6.144.137	80
72.7923910618	Sandbox	172.217.10.35	80
72.7955551147	Sandbox	172.217.10.35	80
72.8021240234	Sandbox	184.26.44.106	80
72.8057091236	Sandbox	23.50.229.108	80
72.8089771271	Sandbox	184.26.44.106	80
72.8222970963	Sandbox	173.222.184.25	80
72.8313760757	Sandbox	66.135.34.17	80

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
72.9932320118	Sandbox	172.217.6.238	80
73.2710211277	Sandbox	172.217.10.35	80
73.3071010113	Sandbox	173.222.184.25	443
73.3075401783	Sandbox	172.217.10.35	443
73.3077201843	Sandbox	172.217.10.35	443
73.3150122166	Sandbox	69.28.187.228	80
73.3907210827	Sandbox	173.222.184.25	443
73.4571890831	Sandbox	173.222.184.25	443
73.6374790668	Sandbox	74.6.144.137	80
73.6534581184	Sandbox	172.217.10.46	80
73.6536941528	Sandbox	104.107.50.14	80
73.6550531387	Sandbox	23.50.229.108	80
74.0218682289	Sandbox	172.217.10.35	443
74.0284891129	Sandbox	72.30.35.9	443
74.0557570457	Sandbox	172.217.10.238	443
74.0569841862	Sandbox	172.217.10.238	443
74.4150512218	Sandbox	172.217.3.110	80
74.4199640751	Sandbox	172.217.3.110	80
74.4344921112	Sandbox	72.21.91.29	80
74.8254070282	Sandbox	172.217.10.238	443
77.4076070786	Sandbox	72.246.43.51	80
89.3972220421	Sandbox	184.26.44.98	80
90.1349041462	Sandbox	104.31.74.124	80
91.2408590317	Sandbox	195.78.120.80	80
96.2055752277	Sandbox	34.198.95.87	80
104.852214098	Sandbox	195.78.120.83	80
105.471423149	Sandbox	23.200.109.88	80
123.3216362	Sandbox	23.67.250.96	80
123.357743025	Sandbox	195.78.120.102	80
123.948339224	Sandbox	23.67.250.107	80
124.828441143	Sandbox	23.67.250.138	80
124.828677177	Sandbox	23.67.250.138	80
124.82885313	Sandbox	23.67.250.138	80
128.163124084	Sandbox	172.217.6.238	80
128.241489172	Sandbox	72.246.43.9	80
128.268465996	Sandbox	52.216.86.35	80
142.484358072	Sandbox	172.217.10.51	80

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
142.525673151	Sandbox	172.217.10.51	80
142.529878139	Sandbox	66.135.34.17	80
142.530930996	Sandbox	104.106.251.24	80
142.564185143	Sandbox	104.106.251.24	443
142.590055227	Sandbox	104.106.251.24	443
142.613391161	Sandbox	104.106.251.24	443
152.566815138	Sandbox	184.26.44.104	80
152.582033157	Sandbox	23.50.229.108	80
152.59475112	Sandbox	172.217.10.46	80
152.933142185	Sandbox	23.50.229.108	80
181.368884087	Sandbox	195.78.120.80	80
185.224830151	Sandbox	54.235.180.144	80
185.292777061	Sandbox	195.78.120.83	80
185.682104111	Sandbox	23.200.109.88	80
186.496842146	Sandbox	23.67.250.121	80
187.253320217	Sandbox	195.78.120.65	80
188.972701073	Sandbox	204.79.197.200	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.10140609741	Sandbox	224.0.0.252	5355
3.12233400345	Sandbox	224.0.0.252	5355
3.12713909149	Sandbox	239.255.255.250	3702
3.15637922287	Sandbox	192.168.56.255	137
5.71235203743	Sandbox	224.0.0.252	5355
6.16526317596	Sandbox	192.168.56.255	138
14.3459801674	Sandbox	224.0.0.252	5355
17.3614611626	Sandbox	224.0.0.252	5355
20.2034490108	Sandbox	8.8.4.4	53
21.0001821518	Sandbox	8.8.4.4	53
24.4069290161	Sandbox	224.0.0.252	5355
25.1249060631	Sandbox	8.8.4.4	53
25.9398801327	Sandbox	8.8.4.4	53
29.6245231628	Sandbox	8.8.4.4	53
29.6870291233	Sandbox	8.8.4.4	53
29.687374115	Sandbox	8.8.4.4	53
29.6956620216	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
29.7850470543	Sandbox	8.8.4.4	53
29.7854130268	Sandbox	8.8.4.4	53
29.7857232094	Sandbox	8.8.4.4	53
30.579349041	Sandbox	8.8.4.4	53
32.4549691677	Sandbox	8.8.4.4	53
32.945674181	Sandbox	8.8.4.4	53
33.0555682182	Sandbox	8.8.4.4	53
33.2405102253	Sandbox	8.8.4.4	53
33.3554031849	Sandbox	8.8.4.4	53
33.3561441898	Sandbox	8.8.4.4	53
33.4017601013	Sandbox	8.8.4.4	53
33.7633631229	Sandbox	224.0.0.252	5355
33.7695991993	Sandbox	224.0.0.252	5355
42.9627120495	Sandbox	224.0.0.252	5355
43.0761930943	Sandbox	224.0.0.252	5355
51.0459861755	Sandbox	8.8.4.4	53
52.3238480091	Sandbox	8.8.4.4	53
53.0132210255	Sandbox	8.8.4.4	53
54.7007751465	Sandbox	8.8.4.4	53
55.1074860096	Sandbox	8.8.4.4	53
56.1075839996	Sandbox	8.8.4.4	53
56.3710260391	Sandbox	8.8.4.4	53
56.3717620373	Sandbox	8.8.4.4	53
56.4528250694	Sandbox	8.8.8.8	53
56.7751610279	Sandbox	8.8.4.4	53
56.7754790783	Sandbox	8.8.4.4	53
56.7828722	Sandbox	8.8.4.4	53
56.7856221199	Sandbox	8.8.4.4	53
56.9720211029	Sandbox	8.8.4.4	53
57.2553241253	Sandbox	8.8.4.4	53
57.2704381943	Sandbox	8.8.4.4	53
57.6121790409	Sandbox	8.8.4.4	53
58.2042322159	Sandbox	8.8.4.4	53
58.4910202026	Sandbox	8.8.4.4	53
58.561453104	Sandbox	8.8.4.4	53
58.9304552078	Sandbox	8.8.4.4	53
58.9507679939	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
59.3680980206	Sandbox	8.8.4.4	53
59.3695361614	Sandbox	8.8.4.4	53
62.6693491936	Sandbox	8.8.4.4	53
62.9600222111	Sandbox	8.8.4.4	53
62.9924931526	Sandbox	8.8.4.4	53
63.3537261486	Sandbox	8.8.4.4	53
65.0668392181	Sandbox	8.8.4.4	53
66.3615221977	Sandbox	8.8.4.4	53
66.3631711006	Sandbox	8.8.4.4	53
67.1128900051	Sandbox	8.8.4.4	53
67.7205510139	Sandbox	8.8.4.4	53
67.8477900028	Sandbox	8.8.4.4	53
67.8482370377	Sandbox	8.8.4.4	53
68.8400230408	Sandbox	8.8.4.4	53
70.5500161648	Sandbox	8.8.4.4	53
72.4437651634	Sandbox	8.8.4.4	53
72.4616341591	Sandbox	8.8.4.4	53
72.5135281086	Sandbox	8.8.8.8	53
72.5301132202	Sandbox	8.8.4.4	53
72.5322780609	Sandbox	8.8.4.4	53
72.7533090115	Sandbox	8.8.4.4	53
72.7536211014	Sandbox	8.8.4.4	53
72.7538881302	Sandbox	8.8.4.4	53
72.7541241646	Sandbox	8.8.4.4	53
72.7543900013	Sandbox	8.8.4.4	53
72.7546620369	Sandbox	8.8.4.4	53
72.7549250126	Sandbox	8.8.4.4	53
73.5976321697	Sandbox	8.8.4.4	53
73.5978751183	Sandbox	8.8.4.4	53
73.5981011391	Sandbox	8.8.4.4	53
73.5983181	Sandbox	8.8.4.4	53
74.0152101517	Sandbox	8.8.4.4	53
74.0156331062	Sandbox	8.8.4.4	53
74.3393452168	Sandbox	8.8.4.4	53
77.1936450005	Sandbox	8.8.4.4	53
89.334788084	Sandbox	8.8.4.4	53
90.0892930031	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
90.9254460335	Sandbox	8.8.4.4	53
96.1515321732	Sandbox	8.8.4.4	53
104.492007017	Sandbox	8.8.4.4	53
105.33714819	Sandbox	8.8.4.4	53
123.259747028	Sandbox	8.8.4.4	53
123.88144207	Sandbox	8.8.4.4	53
124.730623007	Sandbox	8.8.4.4	53
128.150742054	Sandbox	8.8.4.4	53
128.151913166	Sandbox	8.8.4.4	53
128.211405993	Sandbox	8.8.4.4	53
128.236609221	Sandbox	8.8.8.8	53
142.474556208	Sandbox	8.8.4.4	53
142.486615181	Sandbox	8.8.4.4	53
152.520824194	Sandbox	8.8.4.4	53
152.530238152	Sandbox	8.8.4.4	53
152.881731033	Sandbox	8.8.4.4	53
176.446149111	Sandbox	224.0.0.252	5355
179.311360121	Sandbox	239.255.255.250	3702
181.150186062	Sandbox	8.8.4.4	53
181.485567093	Sandbox	224.0.0.252	5355
183.884124994	Sandbox	224.0.0.252	5355
184.058592081	Sandbox	224.0.0.252	5355
185.149598122	Sandbox	8.8.4.4	53
185.170979023	Sandbox	8.8.4.4	53
185.556307077	Sandbox	8.8.4.4	53
186.449442148	Sandbox	8.8.4.4	53
186.612505198	Sandbox	224.0.0.252	5355
187.128038168	Sandbox	8.8.4.4	53
188.947293997	Sandbox	8.8.4.4	53
189.186283112	Sandbox	224.0.0.252	5355
191.734746218	Sandbox	224.0.0.252	5355
194.315817118	Sandbox	224.0.0.252	5355

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\BitTorrentBar2\Rss\Http___news_google_nl_news_cf=All&Ned=Us&Hl=En&Topic=H&Num=3&Output=Rss.Xml.Tmp	**Type :** HTML document, ASCII text, with very long lines **MD5 :** 16a323e4079efe52170b7e98251221c4 **SHA-1 :** b58352cdf991b0f9273b6480072c05ea49ce2640 **SHA-256 :** ad073604b0d75f2ee1e2087622ff453c7da73516 **SHA-512 :** d5a82f2cc6357f3f8d30676aeb5f315941fe229f88 **Size :** 775.69 Kilobytes.
C:\Users\User\AppData\LocalLow\BitTorrentBar2\Rss\Http___rss_cnn_com_rss_cnn_latest_rss.Xml	**Type :** XML document text **MD5 :** d641e69c175f3569cc5224f0ae6c8532 **SHA-1 :** bdb60a90bbd7ba9e06a0c3e5b85214a6365e88b5 **SHA-256 :** 9ea7b89c98c1aea877c001f244d914227a19b66c **SHA-512 :** ff2bfea54166e15e44f8feabfe611a190db81020e6 **Size :** 151.489 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsu28B7.Tmp\Truste_setup.Bmp	**Type :** PC bitmap, Windows 3.x format, 49 x 67 x 24 **MD5 :** 7dad5f1ce516dab93e03984c69ead67b **SHA-1 :** 8d41b1e975e48570d4322573601741a0a9592f06 **SHA-256 :** 5660638da026bcab9e4c016b53a748976a4fb7f0 **SHA-512 :** bee5dd5b794fc3a5158a912b3a28c211e8930ee7 **Size :** 9.97 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsu28B7.Tmp\PublisherLogoDefault.Bmp	**Type :** PC bitmap, Windows 3.x format, 240 x 100 x 8 **MD5 :** 34ab06f8925e32be2b7f6e5faaf3f9af **SHA-1 :** cccbef48cb0dc9cdeebf23adf69aa9c80521d623 **SHA-256 :** f7e42e7eeaa0dfb3392d6fbad5315a8be5464bc0 **SHA-512 :** 3fc901f6f910f0b0ae701976666d4006a432e4cf5a **Size :** 24.136 Kilobytes.
C:\Users\User\AppData\LocalLow\BitTorrentBar2\TbBit1.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 3eb411149b29c5854da31c3c5d3c823f **SHA-1 :** 594e0844207add0dbd163e1afb7696baa25cb961 **SHA-256 :** 95c4201d1d9cb8d5924548a2902621353f876244 **SHA-512 :** e1bd4c13c0cc49979f711e86fef77f42a1f74c497d **Size :** 3236.128 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsu5EAA.Tmp.ToolbarService.Exe	**Type :** PE32 executable (console) Intel 80386, for MS Windows **MD5 :** be4d8d4c01b655ca06acfef1d20b8168 **SHA-1 :** fdf4adb3654ac8e84a67513864636a36359c2b31 **SHA-256 :** d87a65313bc1b48ceea554ad003edb794715186 **SHA-512 :** fa79b4add24dd6105c53101357d213cf7afa4eb4 **Size :** 350.496 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Scorecardresearch[1].Txt	**Type :** ASCII text **MD5 :** 78ffcee742749b0853e4d20a1c468e34 **SHA-1 :** 18249ee8ddd32c79a937b8785edf482df1f561cf **SHA-256 :** 7f96be4a1f8fccd0a82b6bc825b88d2b9ce46691b **SHA-512 :** 1d27def5d1d798b7fb9fbc2fb663d891565b8aa8 **Size :** 0.114 Kilobytes.
C:\Users\User\AppData\LocalLow\BitTorrentBar2\Rss\Http___feeds_reuters_com_reuters_topNews.Xml	**Type :** XML document text **MD5 :** ac7571b2b50d38586886fdeca60b13c5 **SHA-1 :** 2d39ac6494b8ae181e2cc1e5151963b348671468 **SHA-256 :** f816ee7565841a6e73ba45d94bd7487b401dd37 **SHA-512 :** 03701b49b82a091b3bb4d8c07ec5e6a63a11398 **Size :** 22.415 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\Animate-Custom[1].Css	**Type :** ASCII text, with CRLF line terminators **MD5 :** ac808bca941bd589d6fcadd666724e00 **SHA-1 :** b51f9319686f9e659457bf38d0b922081549c701 **SHA-256 :** e1527abc6da6cc596ed9a1cb181682161040950c **SHA-512 :** e3e19fb5505f3edfef421a7f701bf5263282e48ec2 **Size :** 11.469 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsf28F7.Tmp.TbBitT.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 3d45f0adf444c9239497923162027417 **SHA-1 :** ebeafe724cb934442795775b3af373c6c25b2f52 **SHA-256 :** 87d4e79cb8517bcb2698208ea682e34cce4dc809 **SHA-512 :** 1119dd21ca9c033d3cfe5c5b5447859ddee02a69 **Size :** 4401.448 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Apps.Tbccint[2].Txt	**Type :** ASCII text **MD5 :** fef364101d7a7e6716c58b4628ef7dc2 **SHA-1 :** 34da83a440082bded5c96700fecc2dfa6bf6f1af **SHA-256 :** 0cb68acf697b497a34d49abcf86f98e40da24ef1a **SHA-512 :** 1edc268a559e0995db61c3abed1e8ae360e2f1fc **Size :** 0.217 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Services.Apps.Conduit[1].Txt	**Type :** ASCII text **MD5 :** 4c1f57acb1f48ff17a81c9ee486a15ea **SHA-1 :** 9eb616c7229e24f59681e8aa1c29b5610d6eb686 **SHA-256 :** 08c4b692e3982a00133d30c2a6a8580bedcf1104 **SHA-512 :** 8393ac7a0c086b1dc0138ca637d89dd2774a9b72 **Size :** 0.226 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsu28B7.Tmp\Setup_top.Bmp	**Type :** PC bitmap, Windows 3.x format, 726 x 101 x 24 **MD5 :** dfc82ca862605fad9f49b709d471b333 **SHA-1 :** f103e2e37aeb722006eb94f5c3384544ce2b371f **SHA-256 :** 837e5fa5e53935779ddb98e1dff3bac342f0c5462 **SHA-512 :** 2ee8708eea45b8e2acb6543113eaa9ef0758e2df **Size :** 220.234 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsu28B7.Tmp\Alerts_icon.Bmp	**Type :** PC bitmap, Windows 3.x format, 19 x 21 x 24 **MD5 :** c4f797bb9543992727b1de0008f5e042 **SHA-1 :** 2abf095ac3ed12ba8b3164d5d0b62d8cc9ce4170 **SHA-256 :** 11a1e21e3f8c92de518cb3c89a79d2e547ec1102 **SHA-512 :** 8d6db84fbdce606d21823f9f8d03f8cfce4f6c6f6c5 **Size :** 1.316 Kilobytes.
C:\Users\User\AppData\LocalLow\BitTorrentBar2\Rss\Http___news_google_nl_news_pz=1&Cf=All&Ned=Nl_nl&Hl=Nl&Topic=H&Num=3&Output=Rss.Xml.Tmp	**Type :** HTML document, ASCII text, with very long lines **MD5 :** be6415826b35f161f2389ee3fb4ddda6 **SHA-1 :** bbd8676db048852caa7bb7316855ccb71a87d9ca **SHA-256 :** a13d60fb76eaa29e8cc6e950ccddd65cd4dc5c40 **SHA-512 :** e3b4be64a8e90c81e9cbc0af48a5546e13159570 **Size :** 775.682 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Search.Conduit[1].Txt	**Type :** ASCII text **MD5 :** d6042df124369a44743ae32133a7c7bd **SHA-1 :** 1bd38976053693e6a4a55917fde781950b7ca580 **SHA-256 :** cd57c440799bd2b4f43ebc529ff8e3c0ee0695a0c **SHA-512 :** acb59ed1bbf970238c2f5f2d1e869db0550eb412 **Size :** 0.161 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Apps.Cpccint[2].Txt	**Type :** ASCII text **MD5 :** 20aba50f202d2e27b5e2c95b342ff25f **SHA-1 :** 02d65a6d463cdccc118f02f6dc1843a841316da7 **SHA-256 :** 3886565aec16a47076f325fc29ca5de38a0f1ed72 **SHA-512 :** 7bc6a21fcf097414a1212f6d16e9575f63e3f925f3 **Size :** 0.218 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Social.Conduit[2].Txt	**Type :** ASCII text **MD5 :** 510c174c238e054101f9285161ab18a5 **SHA-1 :** eb12d39fcc414397b12895403db933aca59c2671 **SHA-256 :** 3de7fb840209b0037dd7ae6b9fd57a4b20e944b8 **SHA-512 :** 8fdce203b49c86d9b6ea8e4909b5b99441709121 **Size :** 0.219 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6FE1609B-3EC0-11E8-9C49-080027CB305F}.Dat	**Type :** Composite Document File V2 Document, No summary info **MD5 :** 1f3a679596b498dda1327928805802ae **SHA-1 :** 3ac4d876f2aa7a157db6761c261ea2480968225c **SHA-256 :** 7aaad7982e049fcc078f943dd3cc00f05ccb9e295 **SHA-512 :** a71a4e0b4e2ea36e427c5474389247457f3f4043 **Size :** 5.632 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Search.Conduit[1].Txt	**Type :** ASCII text **MD5 :** 7d5e3490b40f0b546dff345ac31e45d9 **SHA-1 :** 0a17281e1803f44739887e681a9e91ad39d7260d **SHA-256 :** a33114fbe950dc9bf47b06a60b3323308782861d **SHA-512 :** ba3f936938d1863a855e7616da8ceb5c585709f9 **Size :** 0.159 Kilobytes.
C:\Users\User\AppData\LocalLow\BitTorrentBar2\Rss\Http___worldpress_org_feeds_topstories_xml.Xml	**Type :** XML document text **MD5 :** ae62af67e41121130c050a0ad248e5b4 **SHA-1 :** 460be5ac36fb9b7bbcef69eaf2190a97c9f7b953 **SHA-256 :** 45b1013514bd9d8505cb36026a8d118b77ce16f2 **SHA-512 :** 581eff053b8adb680e4c9afd43a92a0f18884703b **Size :** 10.237 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Storage.Stgbssint[1].Txt	**Type :** ASCII text **MD5 :** 8a3bf852dee21728d1ad612007ad6f5e **SHA-1 :** 8ba4df6fd292bb445a6be9f24bfe9548e8709a96 **SHA-256 :** a7dc13dc9779946038565169c9b30716da2f2672 **SHA-512 :** e2dd0a3dd2b4a5827e1cfc8f1bd96eb09e2f4058f **Size :** 0.359 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Social.Tbccint[1].Txt	**Type :** ASCII text **MD5 :** 9ea5315f29c2c34c355b7a2cf7a3db58 **SHA-1 :** 03f66ddb908403aa25c68009bf9696bda9cf38c6 **SHA-256 :** 8b8efd9513dd27df7447c49598977496310a1bba **SHA-512 :** d8447506ad0445092accba31f21b60eac6e96505 **Size :** 0.219 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Storage.Stgbssint[2].Txt	**Type :** ASCII text **MD5 :** 02e9ad773c60fcff339fc93c478d72f3 **SHA-1 :** b81bdf32f3966660b0150a0461064a5d8d7dab08 **SHA-256 :** 6799673247158e976d2a74410d558afd6d20c58a **SHA-512 :** e48fc9cbc771553488f5a56d62efd1bb20821c44b **Size :** 0.357 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Storage.Stgbssint[2].Txt	**Type :** ASCII text **MD5 :** 810d9ae1da794069ca62bb3526f8e743 **SHA-1 :** 6b43b317b70a5f3e003c2736fdd4af5d82f129b4 **SHA-256 :** e1965664edf8f1f53647868e3665791b5868e954 **SHA-512 :** ebd04e9ab4827a7957483e46643d299de7c87eb **Size :** 0.219 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsu28B7.Tmp\Search_icon.Bmp	**Type :** PC bitmap, Windows 3.x format, 20 x 18 x 24 **MD5 :** fa93f4e50e397208dbe6da745cec0c57 **SHA-1 :** 3abb3039a4da9a2571df06d4408b1301e394e26e **SHA-256 :** 16d8cd6bb34d0295db30a18e12bb3a4220f2b3e **SHA-512 :** b54e25bda3eae8d387cd618b4c6c64a4f70465fd **Size :** 1.136 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Nsu28B7.Tmp\NsDialogs.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 4ccc4a742d4423f2f0ed744fd9c81f63 **SHA-1 :** 704f00a1acc327fd879cf75fc90d0b8f927c36bc **SHA-256 :** 416133dd86c0dff6b0fcaf1f46dfe97fdc85b37f90e **SHA-512 :** 790c5eb1f8b297e45054c855b66dfc18e9f3f1b18 **Size :** 9.728 Kilobytes.
C:\Users\User\AppData\LocalLow\BitTorrentBar2\Rss\Http___rss_cbc_ca_lineup_latest_xml.Xml	**Type :** XML document text **MD5 :** ec2d7478cc9c7bc4de86718bf62b28b3 **SHA-1 :** fc5961dcad690731db35803d172b61abf3954482 **SHA-256 :** 64b7b9ee01e9e686ffc88b4d149746155041dd69 **SHA-512 :** 92fe579706eb0cc8d59cd29ec6ffb0f934bf90cc07 **Size :** 5.038 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Services.Apps.Tbccint[1].Txt	**Type :** ASCII text **MD5 :** e2e5857dbdcf47603d13404072f51297 **SHA-1 :** 5c8429c5276087f3c6dc0e74c54a16599e965e84 **SHA-256 :** bfaae2274e439b517db5f33d5f128bd59573cd58 **SHA-512 :** 5fb610209f628a30bc5cdaf702c99530c272805b3 **Size :** 0.226 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Services.Apps.Conduit[2].Txt	**Type :** ASCII text **MD5 :** ae40cebdfb5bec847a119f467eb26be1 **SHA-1 :** 55139d66497b7c0b38a41e7caff0aa4ff38b4c00 **SHA-256 :** d373f5d6bf39239c52acf69b1e1ac4c955353c3d9 **SHA-512 :** 84fd1d31e55f3dfcf7a093d639563dcb143e84302 **Size :** 0.226 Kilobytes.
C:\Users\User\AppData\Local\Temp\BitTorrentBar2\Nsj4AA4.TbBit0.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** d2b7c6c7f95030e66500a15489542adb **SHA-1 :** 7148ac44c7fe0cb8d30a12acb28171ae1f609c20 **SHA-256 :** 742be6154a9de7cb52de8d78edccd3333cd7cfe7 **SHA-512 :** 4ecca9abb811998cdc28b57b5253fe75236e3669 **Size :** 5371.168 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Storage.Stgbssint[2].Txt	**Type :** ASCII text **MD5 :** dd69b85c178d98e1383a767426202446 **SHA-1 :** 420f4274b8a7d0ec7bf9ec6357cef6960700dbba **SHA-256 :** 983e9f67ebfb0bd02111eb91a58244dacacec4f22 **SHA-512 :** 8c42dfc3fdd6f662fa152f24da64beb23a141ca422 **Size :** 0.357 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Apps.Conduit[1].Txt	**Type :** ASCII text **MD5 :** 691e5723d174d8e55ce0f99e01816db2 **SHA-1 :** a4846647bf393f19b21558d15af90388000b311e **SHA-256 :** 46703bb9be2b2a0ff07e9fa108a15c5952fb6cf848 **SHA-512 :** dfcf623df586ac4f503a3d706b5eda0dbd4be9cc3 **Size :** 0.217 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Services.Apps.Tbccint[2].Txt	**Type :** ASCII text **MD5 :** 851db8fb1f6755af5d0d2d581e904898 **SHA-1 :** e1a00c5f0f67e8e8aa795b28d6d2ecbc1ef1837b **SHA-256 :** af065007c6a9d6ee855d956d595828d34312391a **SHA-512 :** 663b7f2175b756c61327d5f6ddf97588433da893 **Size :** 0.226 Kilobytes.
C:\Users\User\AppData\LocalLow\BitTorrentBar2\Rss\Http___feeds_news_com_au_public_rss_2_0_news_breaking_news_32_xml.Xml	**Type :** XML document text **MD5 :** abed9037e1f5337b08965b67c21f0184 **SHA-1 :** 57165cc37f9f23abc112dd142743c981a8ff77d0 **SHA-256 :** 14c09941fd04ec1ba2e8505dcff0369155b360382 **SHA-512 :** d157bb0977656a3c385cb72e19895d85088c03d2 **Size :** 16.549 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Social.Tbccint[2].Txt	**Type :** ASCII text **MD5 :** 36a382b6efd034cde94d466fa355be68 **SHA-1 :** 977f6631c93ed098ecebf875f056591c38ee89cc **SHA-256 :** 82f59bba07e5d1c1dc1cc76e93b4311cc6f2ac609 **SHA-512 :** 8218dac36e7d4253b4233639e80e0bebd9f6624 **Size :** 0.219 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsu28B7.Tmp\Home_icon.Bmp	**Type :** PC bitmap, Windows 3.x format, 24 x 20 x 24 **MD5 :** 8a0c3378d7c31243c0b2263224d7e3d5 **SHA-1 :** 072e222c1e42302c33e366d0b272a7b8e87f9434 **SHA-256 :** 56df65c805ae5b7ccaf1cb8ae871475998cb30af4 **SHA-512 :** 422d682d52c980adb8e530dcac88d692021c1e8 **Size :** 1.496 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Apps.Conduit[2].Txt	**Type :** ASCII text **MD5 :** d5b0926fc07e6c75c5792bc5e3f6fcae **SHA-1 :** 4790bb337ca99c196d54cf31b120d26dea1fa2a2 **SHA-256 :** 95987382f099b3f74308d331559aac226093e14c **SHA-512 :** 9c5bbaa96098d48729975aead2191a00c501a14 **Size :** 0.218 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Storage.Stgbssint[1].Txt	**Type :** ASCII text **MD5 :** 43d220f0145ac925a51c5ac0e1cd9829 **SHA-1 :** c8d5bb20ac8151c4d5a3ad05781fbc09e9c52266 **SHA-256 :** 8890e3784ef8587caf3a406e9b998406a5fd3a1ff **SHA-512 :** 84fec8750fb0f2f11868f548de06b62e97eb735fd **Size :** 0.358 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Search.Conduit[3].Txt	**Type :** ASCII text **MD5 :** 2e24ba599b9ee5afb29b7de6b134b81a **SHA-1 :** 9c1493baceadddb058fc8a362832b9b3b2a362a7 **SHA-256 :** f6993d23e7fe10d7f244a866757a317b1917853d **SHA-512 :** 132ef9b39cd6e0508d452686bbd6ac3f941cafcaa **Size :** 0.164 Kilobytes.
C:\Users\User\AppData\LocalLow\BitTorrentBar2\Rss\Http___news_google_nl_news_cf=All&Ned=Fr&Hl=Fr&Topic=H&Num=3&Output=Rss.Xml.Tmp	**Type :** HTML document, ASCII text, with very long lines **MD5 :** 8f3365cfac1d758ff703bdce27bb9f5d **SHA-1 :** 4fdf61257e04816fe897826f6106e64bb12f80a0 **SHA-256 :** 419fa283337ac0abab620dc1e8566aaa384882ce **SHA-512 :** 87d08ddb593400876437b0f358ac9f4b6afd00b0 **Size :** 774.666 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsu28B7.Tmp\System.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** bf712f32249029466fa86756f5546950 **SHA-1 :** 75ac4dc4808ac148ddd78f6b89a51afbd4091c2e **SHA-256 :** 7851cb12fa4131f1fee5de390d650ef65cac56127 **SHA-512 :** 13f69959b28416e0b8811c962a49309dca3f048a **Size :** 11.264 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Apps.Tbccint[1].Txt	**Type :** ASCII text **MD5 :** dd4edd773ae1b7a3ce1e9b8e9142b586 **SHA-1 :** 0ee3eb7b79c7e888e83c9484064ee202b259fc7c **SHA-256 :** 518521acd8a9e8565214843fcb40f1497f7fe95e4 **SHA-512 :** cb9d5ca653de5ff2dd839185e87c67367331b4f7f **Size :** 0.217 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Apps.Cpccint[1].Txt	**Type :** ASCII text **MD5 :** 7734b88de8c303d11005adfdb21cdd26 **SHA-1 :** 34164ee2a181064b212ada405b9d5e261cd87941 **SHA-256 :** 1c94fd873d7b1c5930856fc53c76da0e1a1175f78 **SHA-512 :** 49dd547f3451da2346b6e86a7165dd8024f5f6cd **Size :** 0.217 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Storage.Stgbssint[1].Txt	**Type :** ASCII text **MD5 :** 404b46ea42005a40deeb2f01cd1ee888 **SHA-1 :** e1b66aa3ae794b2443189c4dd9a92eaf72efb7d2 **SHA-256 :** 22dca975d26430425d8b51d3438228361fca15b6 **SHA-512 :** 9286453baa2301d1719020437794f1895b1ef4d4 **Size :** 0.124 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Search.Conduit[3].Txt	**Type :** ASCII text **MD5 :** b7e47ff29dbee82cb8297cb56e79fbe6 **SHA-1 :** 24320350033b96ed499b1bebeb498fc1c40697f6 **SHA-256 :** d988154e340671121956b784455c0de8d0d4c85 **SHA-512 :** 7fa1094b8dea5f9f1f7692c93492f6ab7a0bc2e20 **Size :** 0.162 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Social.Conduit[1].Txt	**Type :** ASCII text **MD5 :** d6e065027bab23ccead87b337a920f4e **SHA-1 :** 8ac5cfbf14d79c28ae97e86f8069bdfc802552e6 **SHA-256 :** aa587fafe0a1f091f8ce74b3490c991320c7de77e3 **SHA-512 :** 68b4bf0083494191405706586c0467dd628985343 **Size :** 0.219 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nsu28B7.Tmp\License.Txt	**Type :** Non-ISO extended-ASCII text, with very long lines, with CRLF line terminators **MD5 :** 7ae4e62f7e0b731a3193abfa2a8a5f44 **SHA-1 :** 8742d66b038c77b5816f05333a199601abf7a22e **SHA-256 :** a18697b6eefe70cfa1d960d4e2edfbe1a7540b7cc **SHA-512 :** 8d2dde55ca6db06de08f026318fd7b5bc6b95dc1 **Size :** 18.9 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nso498A.Tmp\NsUtils.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 171ba3288223173eb5a1a5e440bb5b89 **SHA-1 :** a262058e83179a203697951bd59772d08cc74878 **SHA-256 :** 4a143646832a887c8b4bbf27a58890f3c4d46bb7 **SHA-512 :** f812668a35cb6df2ca5b7ef09deeb3a18341bd38(**Size :** 314.656 Kilobytes.
C:\Users\User\AppData\Local\Temp\Nso498A.Tmp\System.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 4cf3a81ab4579b30117c8a39a489d51d **SHA-1 :** 61af475e11e4e79e6a11e761fcb540d9c5eec0e9 **SHA-256 :** 29f4a1c87161643e0ed5c46b46786d9a48437ec5 **SHA-512 :** 885d131304afbe92b9b0a16830b6b34c6b78e44f **Size :** 11.264 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\F[1].Txt	**Type :** ASCII text, with no line terminators **MD5 :** 4c92b20a326d48c29f3fdeacec413f28 **SHA-1 :** f5ad31b21386e81e2e0fe12e5762bab39ddef710 **SHA-256 :** be04ee6479e67725d2dcd744cdacd0cc551e96d3 **SHA-512 :** 5c9e3c8ee1a358be381e70800fef5f73820e70086 **Size :** 0.115 Kilobytes.
C:\Users\User\AppData\LocalLow\BitTorrentBar2\Plugins\{5E1360DC-8FA8-40df-A8CD-FC3831B3634B}\{5E1360DC-8FA8-40df-A8CD-FC3831B3634B}.Cpi	**Type :** Microsoft Cabinet archive data, 178858 bytes, 3 files **MD5 :** 2593ae0f033d5bceb23969e71ba8b50a **SHA-1 :** 3e694845dc53f08ac299ca23da974c55f4b62e20 **SHA-256 :** 36420a4e62b637498c58938a38d79af45b05cd21 **SHA-512 :** bbcbe6aa6f644d00d219d727589384377ae58d0 **Size :** 186.578 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Nsu28B7.Tmp\License_uni.Txt	**Type :** Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators **MD5 :** a63efffef7d089e0a4eb20aef0de7ebf **SHA-1 :** 24f5b721baff744495bf9fd2acf3d9ce80551e49 **SHA-256 :** 3678571ed7e5474dec2cefe9721d7449f8fb807bc **SHA-512 :** ada164c596a95e111eacbf47e47f7d34a4fc83e88 **Size :** 37.942 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	None
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	267ef53ea1a203e5181a3ab0d7ad860085834b19
MD5:	4693fd2fba5e6d8a8c15699152edddaf
First Seen Date:	2018-04-12 00:15:41.240484 (about a year ago)
Number Of Clients Seen:	2
Last Analysis Date:	2018-08-07 15:15:17.355397 (11 months ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	6
Trid	[[41.0, u'Win32 Executable MS Visual C++ (generic)'], [36.3, u'Win64 Executable (generic)'], [8.6, u'Win32 Dynamic Link Library (generic)'], [5.9, u'Win32 Executable (generic)'], [2.6, u'OS/2 Executable (generic)']]
Compilation Time Stamp	0x4F47E2DA [Fri Feb 24 19:19:54 2012 UTC]
LegalCopyright	Conduit Ltd.
FileDescription	BitTorrentBar2 Toolbar
FileVersion	6.8.11.4
CompanyName	Conduit
Translation	0x0000 0x0000
Entry Point	0x403883 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	2151456
Ssdeep	
Sha256	39a8831ca5858e191ca1da41b6d065145e9daf05e1351ca45c6ed15d6c7452ee
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	be41bf7b8cc010b614bd36bbca606973

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x6dae	0x6e00	6.50852956314	00499a6f70259150109c809d6aa0e6ed
.rdata	0x8000	0x2a62	0x2c00	4.39053502099	07990aaa54c3bc638bb87a87f3fb13e3
.data	0xb000	0x67ebc	0x200	1.43086025975	014871d9a00f0e0c8c2a7cd25606c453
.ndata	0x73000	0x329000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x39c000	0xe40	0x1000	4.10848221943	b8053a3ea607bb216bdbb83103a4fef9
.reloc	0x39d000	0xf32	0x1000	5.0350036709	1773d06731e6b6560afc389d53b9ae5c

PE Imports

- KERNEL32.dll
  - SetFileTime
  - CompareFileTime
  - SearchPathW
  - GetShortPathNameW
  - GetFullPathNameW
  - MoveFileW
  - SetCurrentDirectoryW
  - GetFileAttributesW
  - GetLastError
  - CreateDirectoryW
  - SetFileAttributesW
  - Sleep
  - GetTickCount
  - GetFileSize
  - GetModuleFileNameW
  - GetCurrentProcess
  - CopyFileW
  - ExitProcess
  - GetWindowsDirectoryW
  - GetTempPathW
  - GetCommandLineW
  - SetErrorMode
  - lstrcpynA
  - CloseHandle
  - lstrcpynW
  - GetDiskFreeSpaceW
  - GlobalUnlock
  - GlobalLock
  - CreateThread
  - LoadLibraryW
  - CreateProcessW
  - lstrcmpiA
  - CreateFileW
  - GetTempFileNameW
  - lstrcatW
  - GetProcAddress
  - LoadLibraryA
  - GetModuleHandleA
  - OpenProcess
  - lstrcpyW
  - GetVersionExW
  - GetSystemDirectoryW
  - GetVersion
  - lstrcpyA
  - RemoveDirectoryW
  - lstrcmpA
  - lstrcmpiW
  - lstrcmpW
  - ExpandEnvironmentStringsW
  - GlobalAlloc
  - WaitForSingleObject
  - GetExitCodeProcess
  - GlobalFree
  - GetModuleHandleW
  - LoadLibraryExW
  - FreeLibrary
  - WritePrivateProfileStringW
  - GetPrivateProfileStringW
  - WideCharToMultiByte
  - lstrlenA
  - MulDiv
  - WriteFile
  - ReadFile
  - MultiByteToWideChar
  - SetFilePointer
  - FindClose
  - FindNextFileW
  - FindFirstFileW
  - DeleteFileW
  - lstrlenW
- USER32.dll
  - GetAsyncKeyState
  - IsDlgButtonChecked
  - ScreenToClient

    - GetMessagePos
    - CallWindowProcW
    - IsWindowVisible
    - LoadBitmapW
    - CloseClipboard
    - SetClipboardData
    - EmptyClipboard
    - OpenClipboard
    - TrackPopupMenu
    - GetWindowRect
    - AppendMenuW
    - CreatePopupMenu
    - GetSystemMetrics
    - EndDialog
    - EnableMenuItem
    - GetSystemMenu
    - SetClassLongW
    - IsWindowEnabled
    - SetWindowPos
    - DialogBoxParamW
    - CheckDlgButton
    - CreateWindowExW
    - SystemParametersInfoW
    - RegisterClassW
    - SetDlgItemTextW
    - GetDlgItemTextW
    - MessageBoxIndirectW
    - CharNextA
    - CharUpperW
    - CharPrevW
    - wvsprintfW
    - DispatchMessageW
    - PeekMessageW
    - wsprintfA
    - DestroyWindow
    - CreateDialogParamW
    - SetTimer
    - SetWindowTextW
    - PostQuitMessage
    - SetForegroundWindow
    - ShowWindow
    - wsprintfW
    - SendMessageTimeoutW
    - LoadCursorW
    - SetCursor
    - GetWindowLongW
    - GetSysColor
    - CharNextW
    - GetClassInfoW
    - ExitWindowsEx
    - IsWindow
    - GetDlgItem
    - SetWindowLongW
    - LoadImageW
    - GetDC
    - EnableWindow
    - InvalidateRect
    - SendMessageW
    - DefWindowProcW
    - BeginPaint
    - GetClientRect
    - FillRect
    - DrawTextW
    - EndPaint
    - FindWindowExW
- GDI32.dll
    - SetBkColor
    - GetDeviceCaps
    - DeleteObject
    - CreateBrushIndirect
    - CreateFontIndirectW
    - SetBkMode
    - SetTextColor
    - SelectObject
- SHELL32.dll

- SHBrowseForFolderW
- SHGetPathFromIDListW
- SHGetFileInfoW
- ShellExecuteW
- SHFileOperationW
- SHGetSpecialFolderLocation

- ADVAPI32.dll
  - RegEnumKeyW
  - RegOpenKeyExW
  - RegCloseKey
  - RegDeleteKeyW
  - RegDeleteValueW
  - RegCreateKeyExW
  - RegSetValueExW
  - RegQueryValueExW
  - RegEnumValueW
- COMCTL32.dll
  - ImageList_AddMasked
  - ImageList_Destroy
  - None
  - ImageList_Create
- ole32.dll
  - CoTaskMemFree
  - OleInitialize
  - OleUninitialize
  - CoCreateInstance
- VERSION.dll
  - GetFileVersionInfoSizeW
  - GetFileVersionInfoW
  - VerQueryValueW

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 3785176, u'sha256': u'fa38c19f3e9ff3140b9a653ac955d2677b857080342bd200120b7447ba662287', u'type': u'data', u'size': 744}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 3785920, u'sha256': u'4d3e102d142256cfff78342a603b41ab4318b5d8a59377e2f7f5dc1b4c723706', u'type': u'data', u'size': 480}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 3786400, u'sha256': u'2bf0937151f0150eaf671e145d86a2a8a986519646c185b7bf95cef23afc014e', u'type': u'data', u'size': 248}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 3786648, u'sha256': u'18466509968c3c0bf92ba410fea075def2b257a5a799a113cbc60f13e75f4b01', u'type': u'data', u'size': 238}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 3786888, u'sha256': u'c914a0ae7093e6d85946fe32540dee4047660be2114a5d823fe8f545b69c2568', u'type': u'MS Windows icon resource - 1 icon, 32x32, 16 colors', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 3786912, u'sha256': u'da549e248424d0596b1f449c02cc1ed14100cb518ead63479f02c61d7453f488', u'type': u'data', u'size': 472}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 3787384, u'sha256': u'dcafe7f3c92e74965a00b611e1cbff922273b3d4a491f079faaa1b4915040d12', u'type': u'XML 1.0 document, ASCII text, with very long lines, with no line terminators', u'size': 968}

CERTIFICATE VALIDATION

- Success ✔

[+] Thawte Timestamping CA	
Status	NoError ✔
Start Date	1997-01-01 02:00:00
End Date	2021-01-01 01:59:59
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Key Identifier	null
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	null
Crl link	null
Key Usage	null
Extended Usage	null

[+] VeriSign Time Stamping Services CA	
Status	NotTimeValid (no effect on chain status)
Start Date	2003-12-04 02:00:00
End Date	2013-12-04 01:59:59
Sha256	179b45497685f7a2004ad57d90497949fb8ec0eef6f4af7ab2fd89582bc712be
Serial	47BF1995DF8D524643F7DB6D480D31A4
Subject Key Identifier	null
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	null
Crl link	http://crl.verisign.com/ThawteTimestampingCA.crl
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	{"Time Stamping (1.3.6.1.5.5.7.3.8)"}

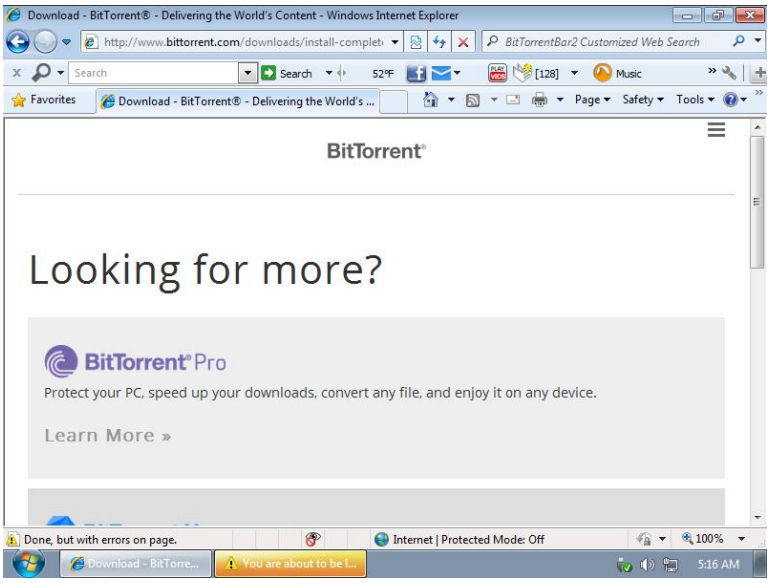
[+] Symantec Time Stamping Services Signer - G3	
Status	NotTimeValid (no effect on chain status)
Start Date	2012-05-01 03:00:00
End Date	2013-01-01 01:59:59
Sha256	1d9ced90ca3230ad654adbaf2776b9fc3ad2c22c81c45ced1af6da4585ed8a63
Serial	79A2A585F9D1154213D9B83EF6B68DED
Subject Key Identifier	b4 b7 f1 89 49 26 60 e7 65 ea 73 ae dc d3 38 cd bf 57 92 6f
Issuer Name	VeriSign Time Stamping Services CA
Issuer Key Identifier	null
Crl link	http://crl.verisign.com/tss-ca.crl
Key Usage	{"Digital Signature (80)"}
Extended Usage	{"Time Stamping (1.3.6.1.5.5.7.3.8)"}

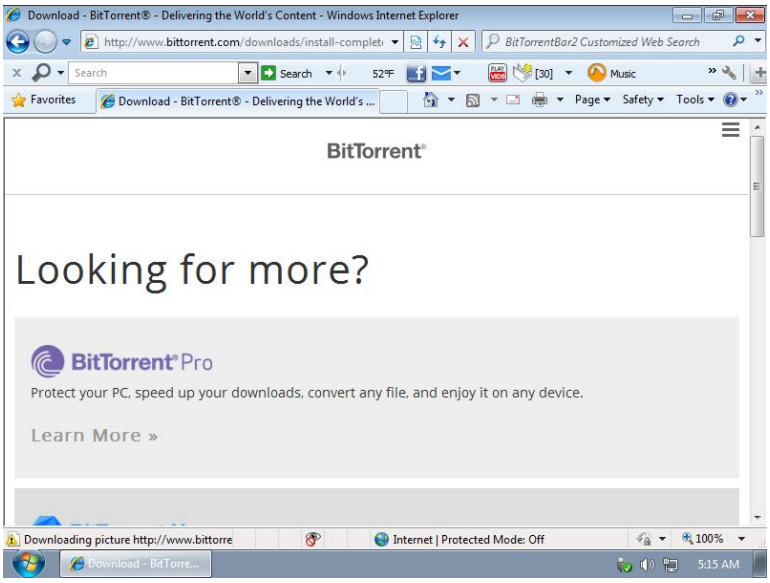
[+] null	
Status	NoError ✔
Start Date	1996-01-29 02:00:00
End Date	2028-08-02 02:59:59
Sha256	069bea1e3945c8d374dc550adc09f71f6c07cbc83df3af204e7bbc1cab4520a8
Serial	70BAE41D10D92934B638CA7B03CCBABF
Subject Key Identifier	null
Issuer Name	null
Issuer Key Identifier	null
Crl link	null
Key Usage	null
Extended Usage	null

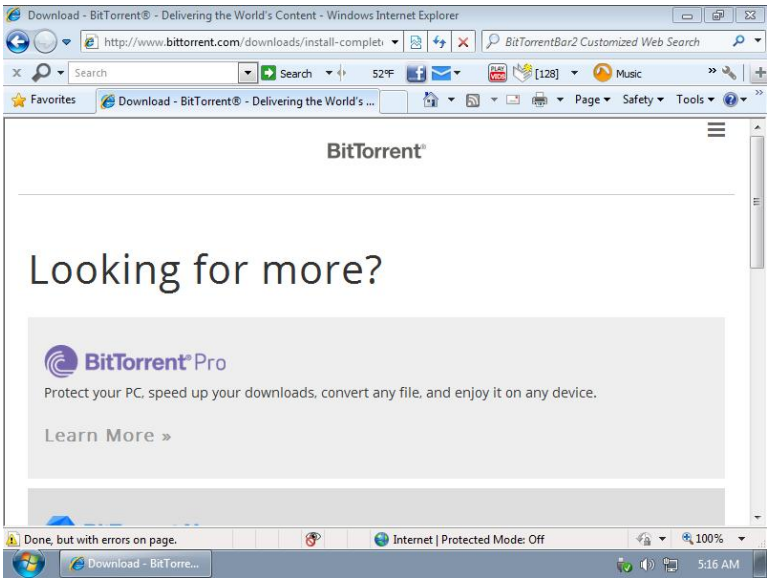
[+] VeriSign Class 3 Code Signing 2009-2 CA	
Status	NoError ✔
Start Date	2009-05-21 03:00:00
End Date	2019-05-21 02:59:59
Sha256	dc7d56b04ee94b6ab175ca9ec837a2894788d77c9fb413354138addfe4ee0be2
Serial	655226E1B22E18E1590F2985AC22E75C
Subject Key Identifier	97 d0 6b a8 26 70 c8 a1 3f 94 1f 08 2d c4 35 9b a4 a1 1e f2
Issuer Name	null
Issuer Key Identifier	null
Crl link	http://crl.verisign.com/pca3.crl
Key Usage	{"Certificate Signing","Off-line CRL Signing","CRL Signing (06)"}
Extended Usage	{"Client Authentication (1.3.6.1.5.5.7.3.2)"}

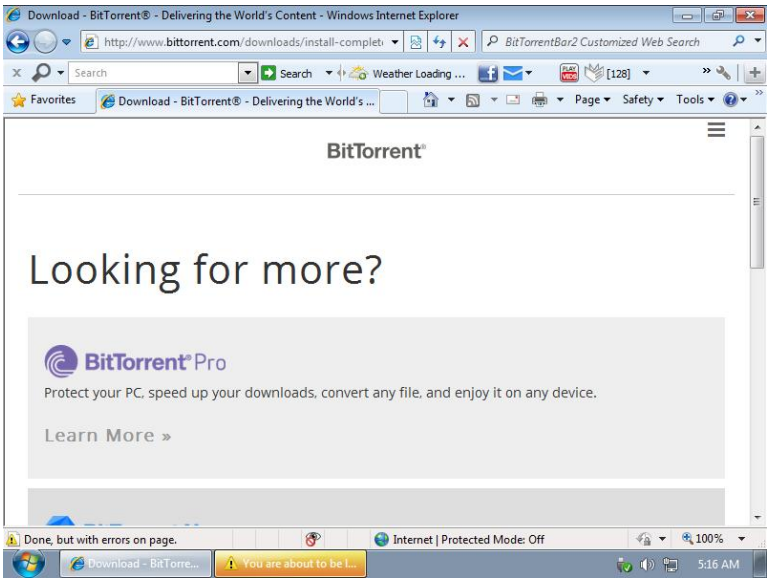
[+] Conduit Ltd.	
Status	NotTimeValid ϟ (no effect on chain status)
Start Date	2010-02-17 02:00:00
End Date	2013-03-30 01:59:59
Sha256	9b4049db0aefc5795720c17dc876bcfcf3404b069f038bdbfdecfd9e47d9d375
Serial	3736DA15AF647632CCE61CD41B6577DD
Subject Key Identifier	null
Issuer Name	VeriSign Class 3 Code Signing 2009-2 CA
Issuer Key Identifier	97 d0 6b a8 26 70 c8 a1 3f 94 1f 08 2d c4 35 9b a4 a1 1e f2
Crl link	http://csc3-2009-2-crl.verisign.com/CSC3-2009-2.crl
Key Usage	{"Digital Signature (80)"}
Extended Usage	{"Code Signing (1.3.6.1.5.5.7.3.3)"}

SCREENSHOTS



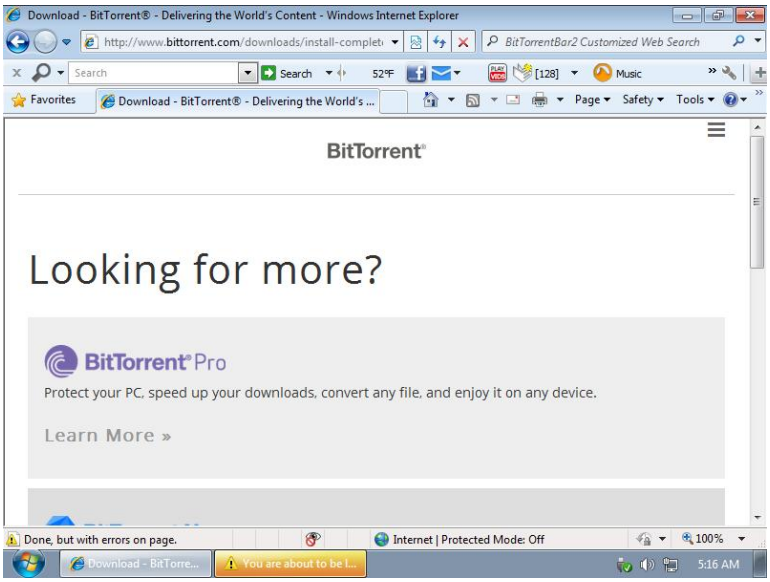


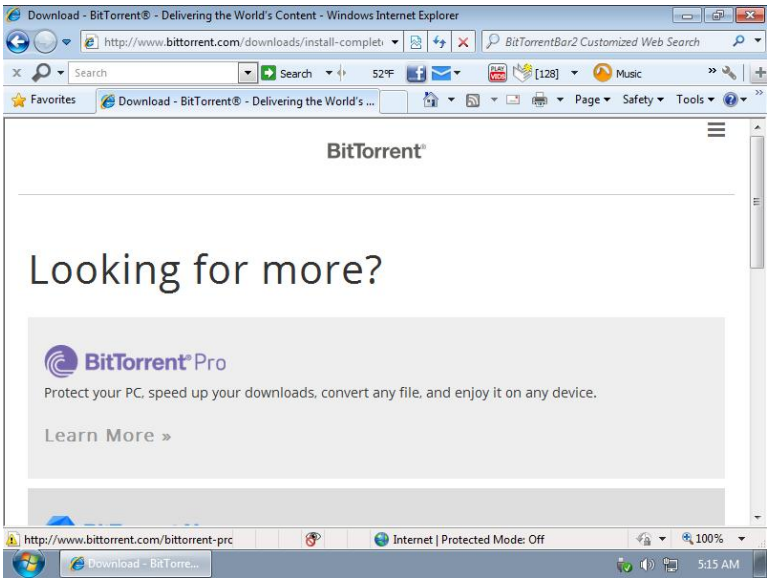


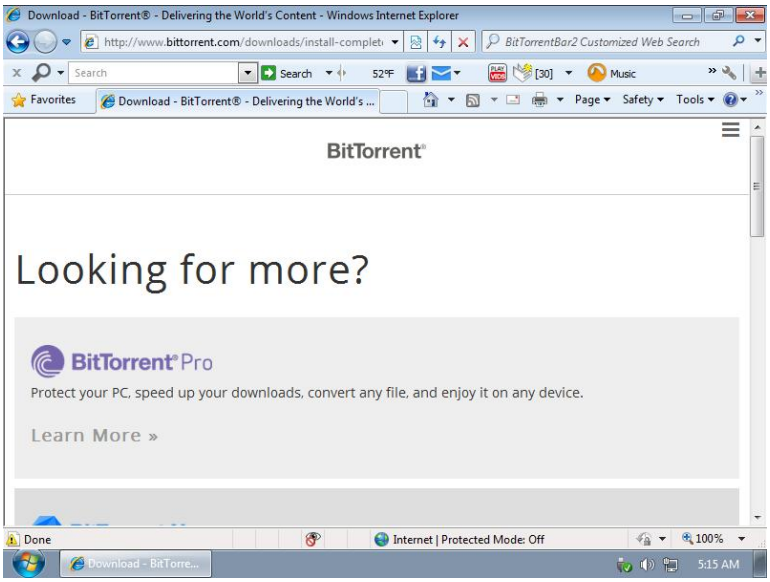

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complet
BitTorrentBar2 Customized Web Search
Search
Weather Loading ...
[128]
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
BitTorrent
Looking for more?
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
Done, but with errors on page.
Internet | Protected Mode: Off
100%
Download - BitTorre...
You are about to be l...
5:16 AM

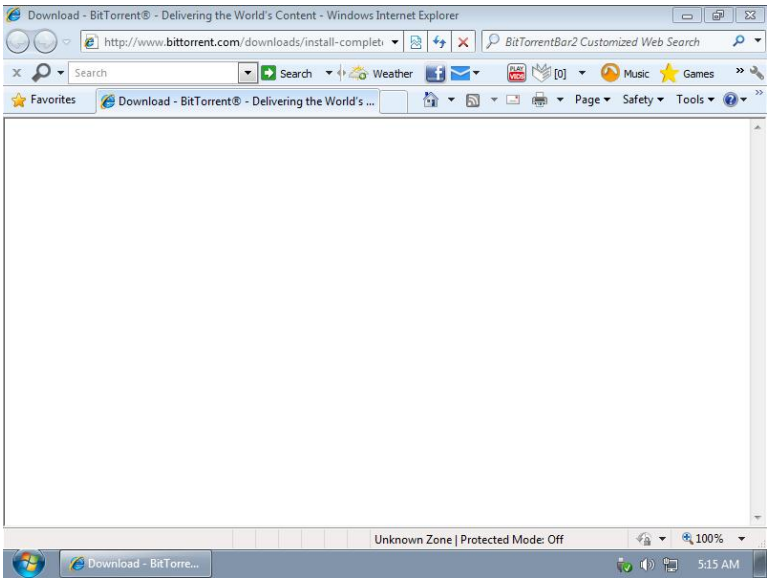

Windows Internet Explorer
Search...

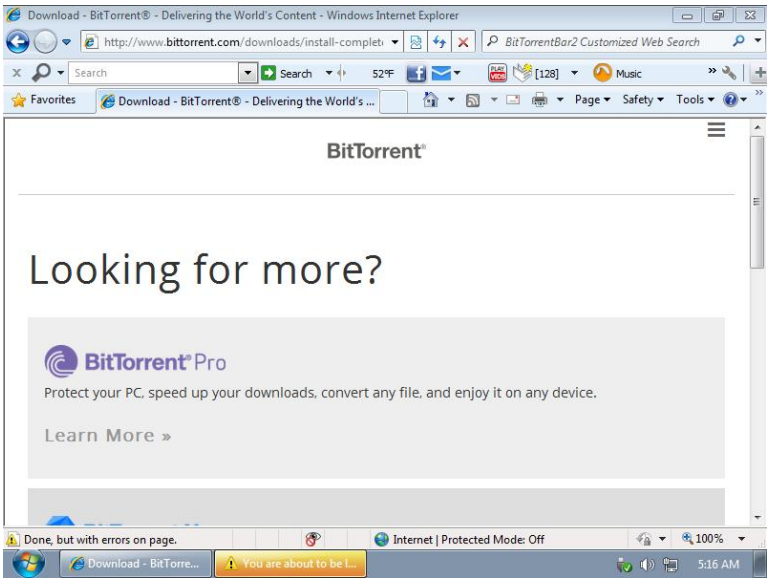

Windows Internet Ex...
5:14 AM

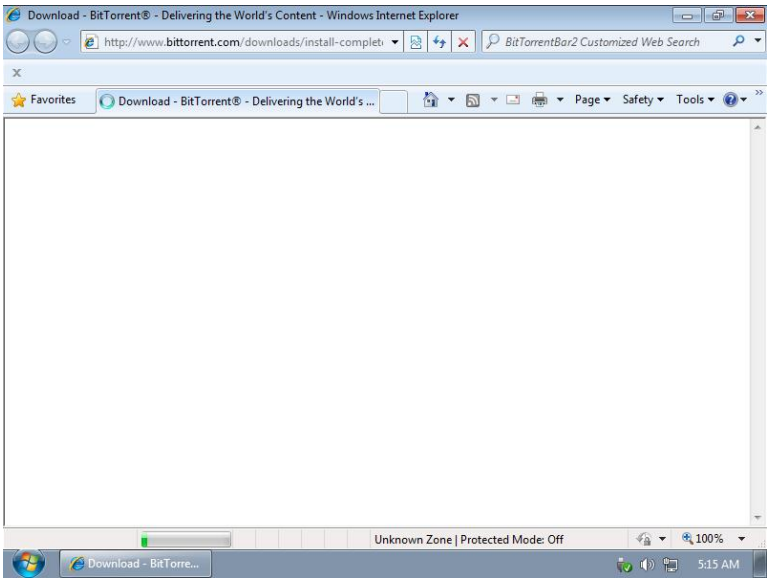

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complet
BitTorrentBar2 Customized Web Search
Search
52°F
[128]
Music
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
BitTorrent
Looking for more?
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
Done, but with errors on page.
Internet | Protected Mode: Off
100%
Download - BitTorre...
You are about to be l...
5:16 AM


Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
BitTorrent
Looking for more?
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
Internet | Protected Mode: Off
100%
5:15 AM

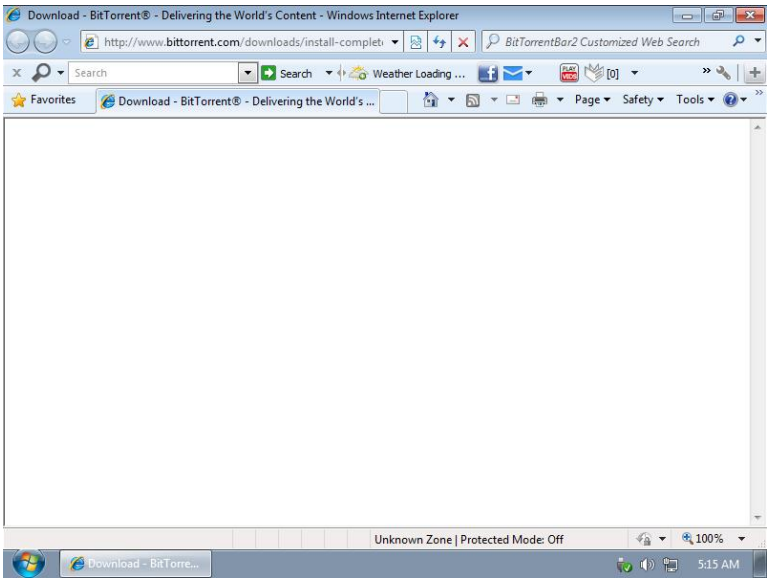

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
BitTorrent
Looking for more?
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
Done
Internet | Protected Mode: Off
100%
5:15 AM

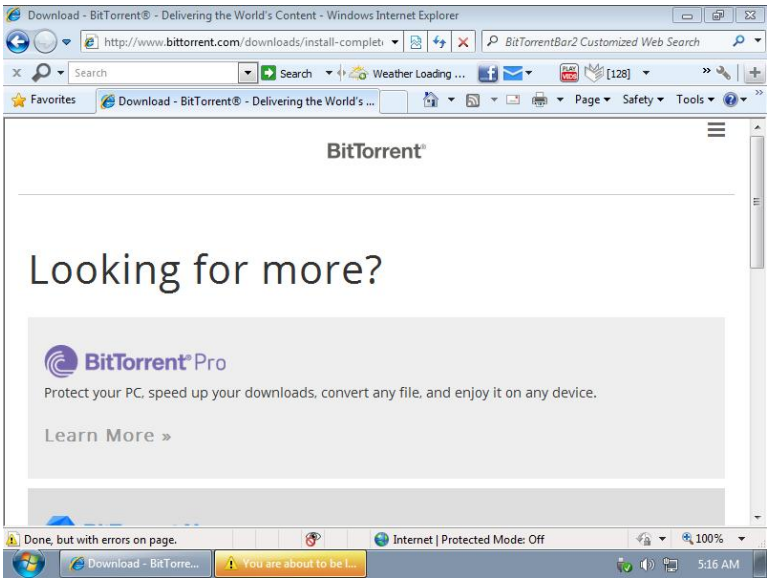

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
Unknown Zone | Protected Mode: Off
100%
5:15 AM

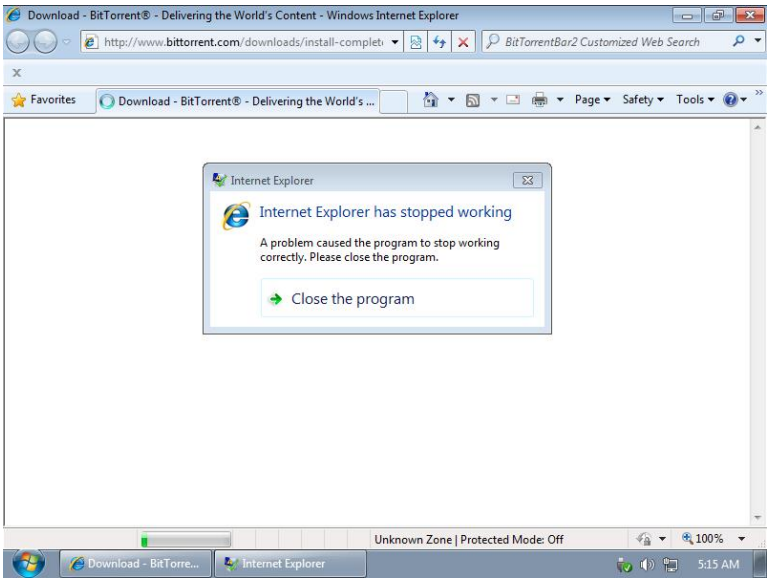

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complet
BitTorrentBar2 Customized Web Search
Search
52°F
[128]
Music
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
BitTorrent
Looking for more?
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
Done, but with errors on page.
Internet | Protected Mode: Off
100%
Download - BitTorre...
You are about to be l...
5:16 AM

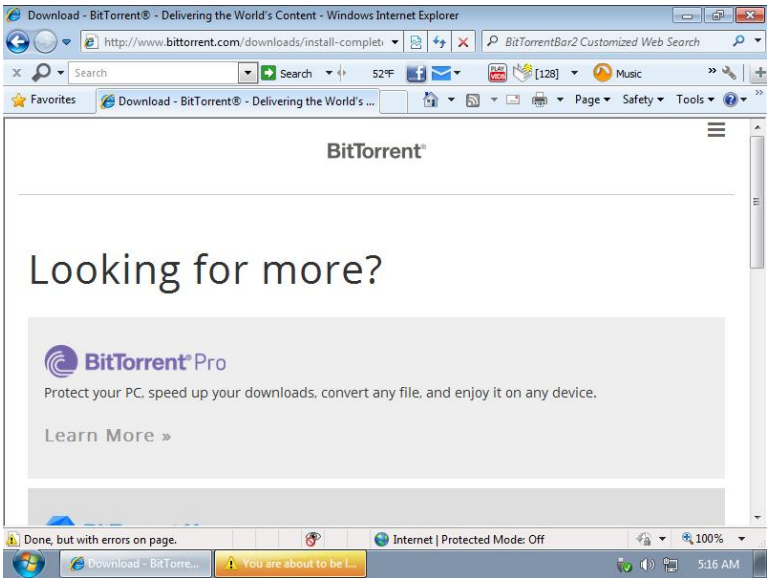

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complet
BitTorrentBar2 Customized Web Search
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
Unknown Zone | Protected Mode: Off
100%
Download - BitTorre...
5:15 AM

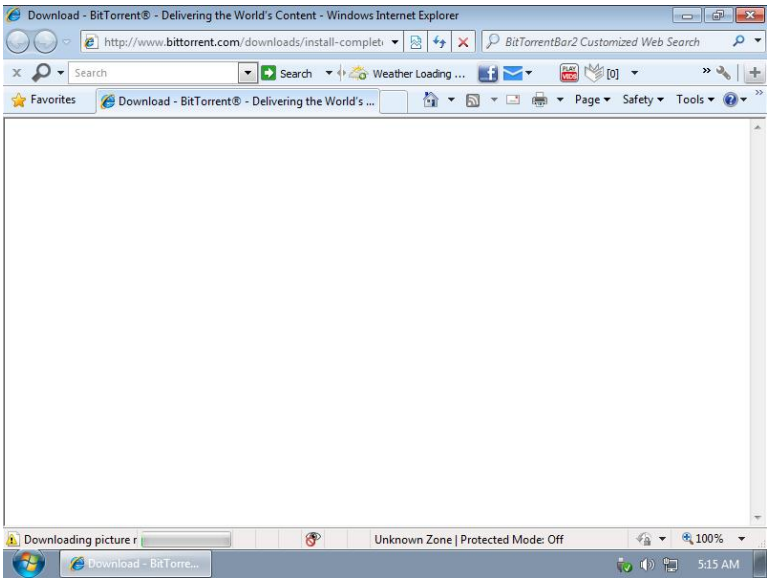

Computer
5:14 AM

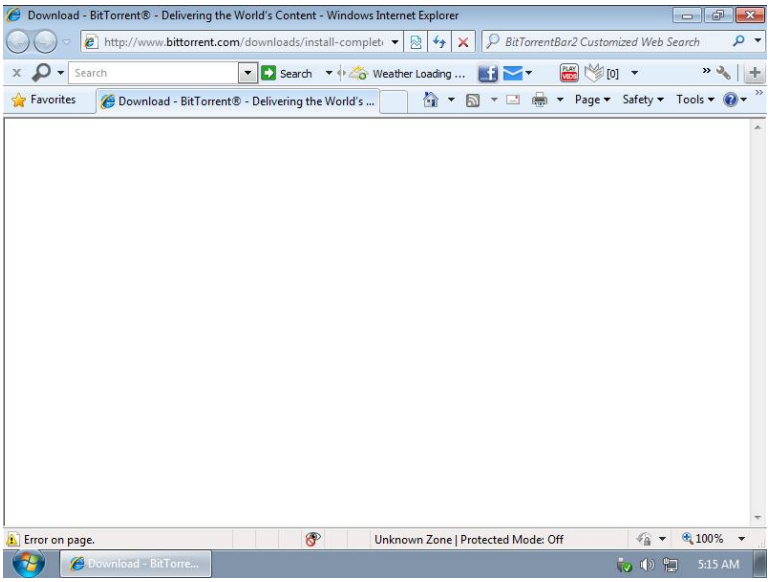

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complete
BitTorrentBar2 Customized Web Search
Search
Weather Loading ...
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
Unknown Zone | Protected Mode: Off
100%
Download - BitTorre...
5:15 AM


Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complete
BitTorrentBar2 Customized Web Search
Search
Weather Loading ...
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
BitTorrent
Looking for more?
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
Done, but with errors on page.
Internet | Protected Mode: Off
100%
Download - BitTorre...
You are about to be l...
5:16 AM

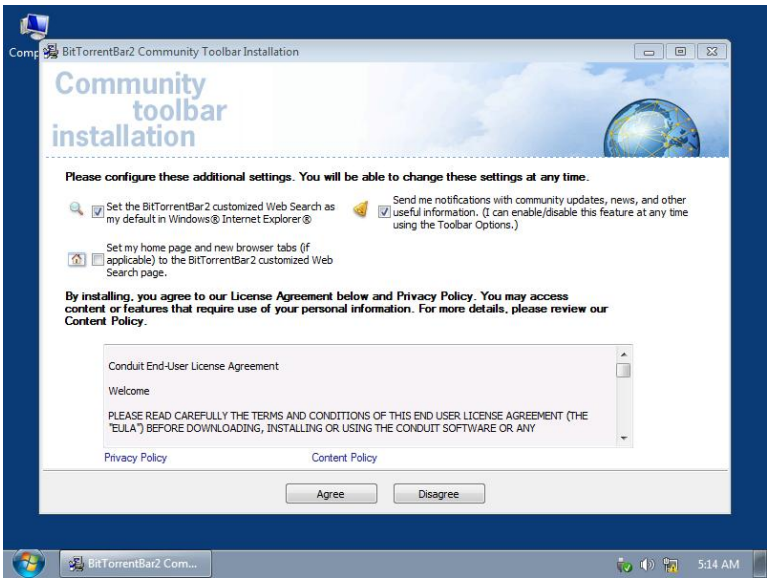

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complete
BitTorrentBar2 Customized Web Search
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
Internet Explorer
Internet Explorer has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
Unknown Zone | Protected Mode: Off
100%
Download - BitTorre...
Internet Explorer
5:15 AM

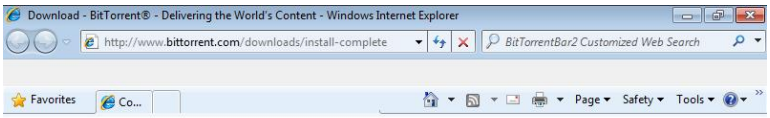

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
BitTorrent
Looking for more?
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
Done, but with errors on page.
Internet | Protected Mode: Off
5:16 AM


Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
Downloading picture r
Unknown Zone | Protected Mode: Off
5:15 AM

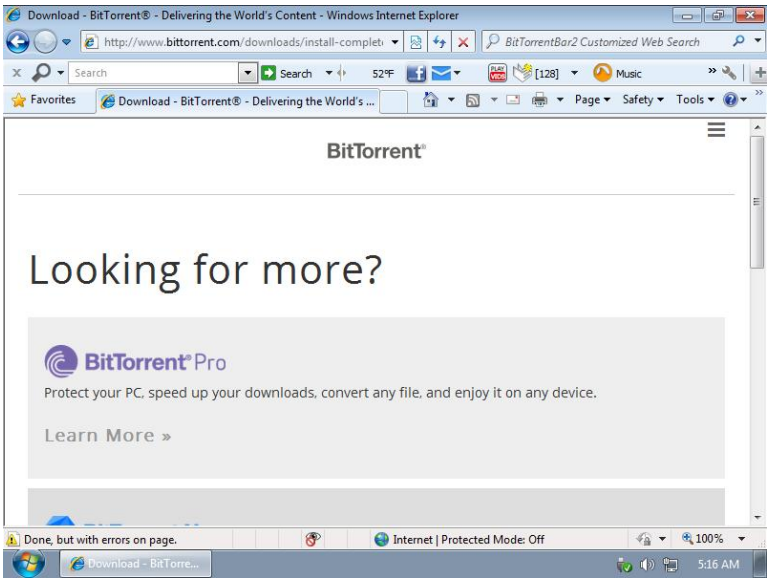

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
Error on page.
Unknown Zone | Protected Mode: Off
5:15 AM

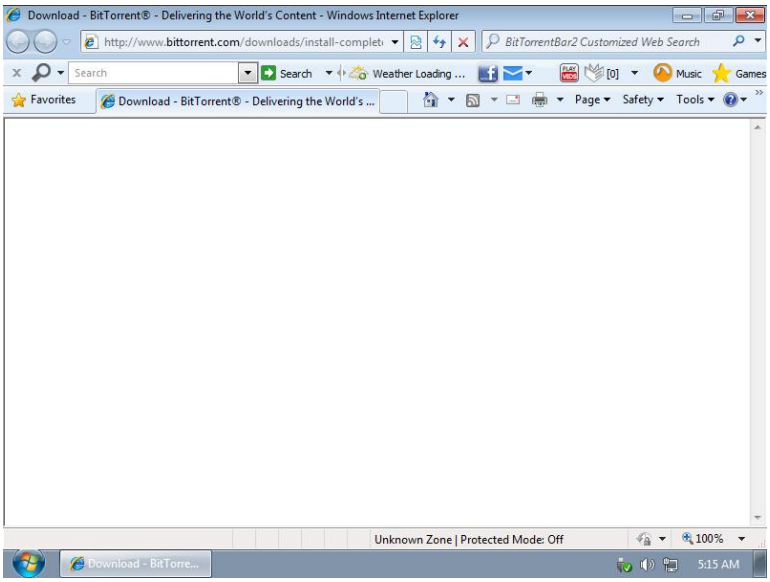

Computer
5:14 AM


BitTorrentBar2 Community Toolbar Installation
Community toolbar installation
Please configure these additional settings. You will be able to change these settings at any time.
Set the BitTorrentBar2 customized Web Search as my default in Windows® Internet Explorer®
Send me notifications with community updates, news, and other useful information. (I can enable/disable this feature at any time using the Toolbar Options.)
Set my home page and new browser tabs (if applicable) to the BitTorrentBar2 customized Web Search page.
By installing, you agree to our License Agreement below and Privacy Policy. You may access content or features that require use of your personal information. For more details, please review our Content Policy.
Conduit End-User License Agreement
Welcome
PLEASE READ CAREFULLY THE TERMS AND CONDITIONS OF THIS END USER LICENSE AGREEMENT (THE "EULA") BEFORE DOWNLOADING, INSTALLING OR USING THE CONDUIT SOFTWARE OR ANY
Privacy Policy
Content Policy
Agree
Disagree
BitTorrentBar2 Com...
5:14 AM

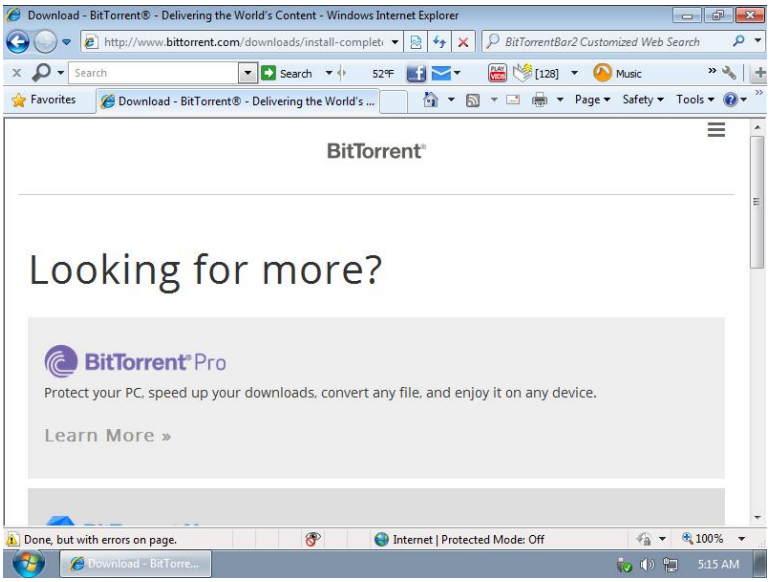

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complete
BitTorrentBar2 Customized Web Search
Favorites
Page
Safety
Tools

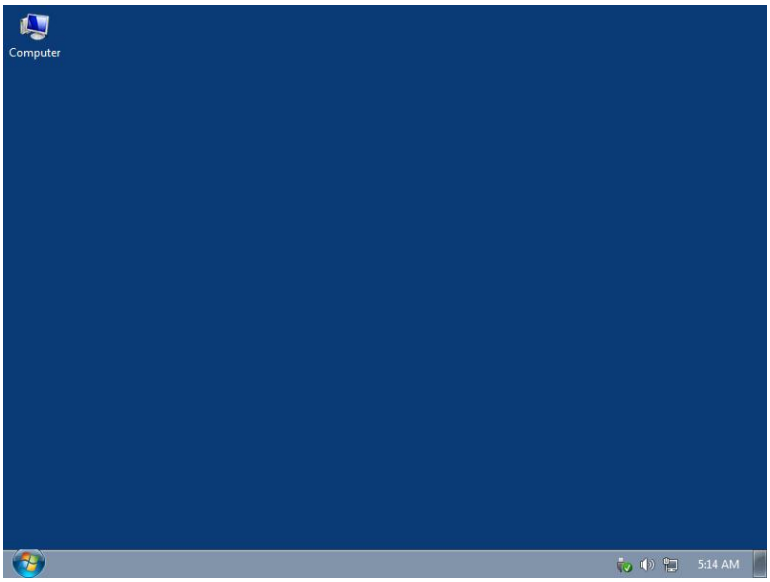

Download - BitTorre...
5:15 AM

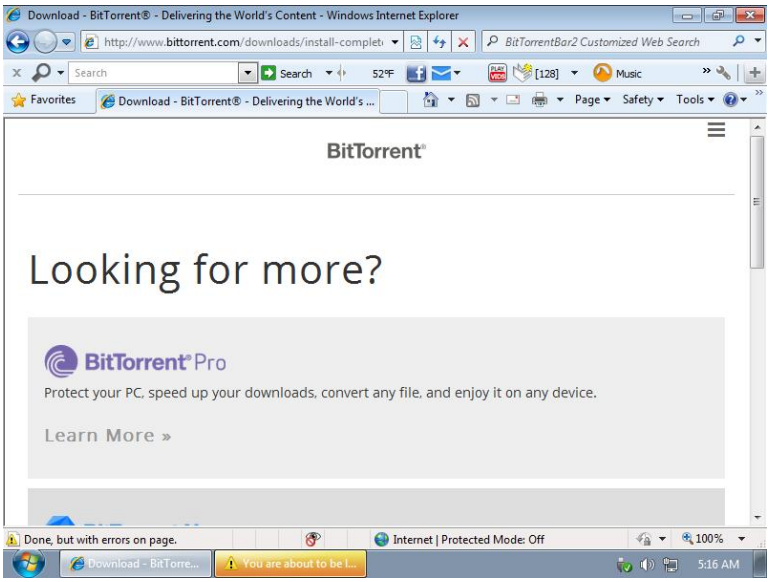

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complete
BitTorrentBar2 Customized Web Search
Search
52°F
[128]
Music
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
BitTorrent
Looking for more?
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
Done, but with errors on page.
Internet | Protected Mode: Off
100%
Download - BitTorre...
5:16 AM

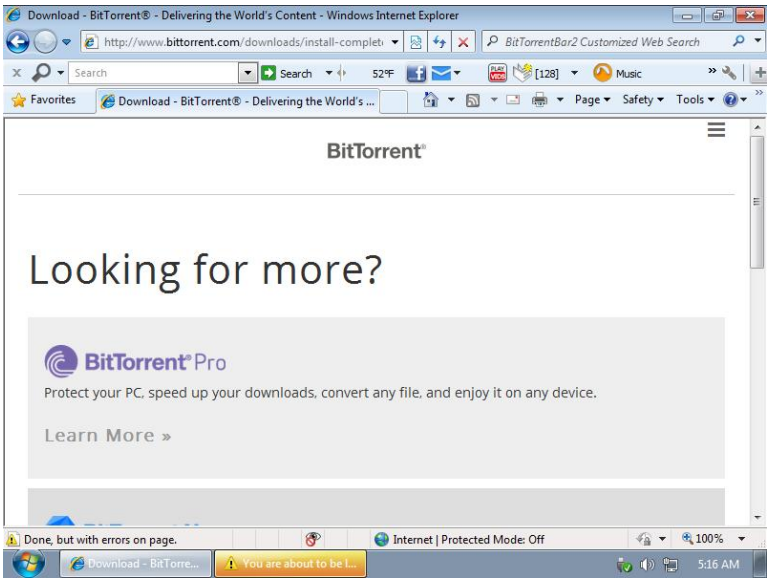

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complete
BitTorrentBar2 Customized Web Search
Search
Weather Loading ...
[0]
Music
Games
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
Unknown Zone | Protected Mode: Off
100%
Download - BitTorre...
5:15 AM

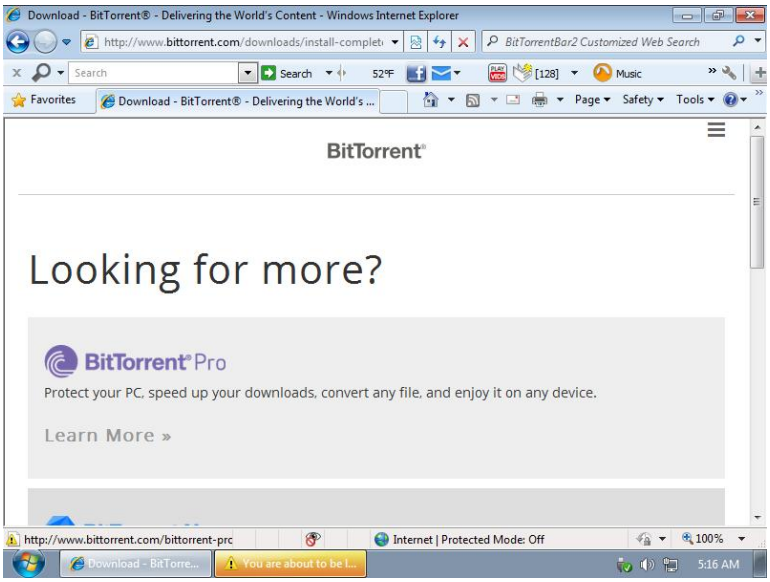

Computer
5:14 AM

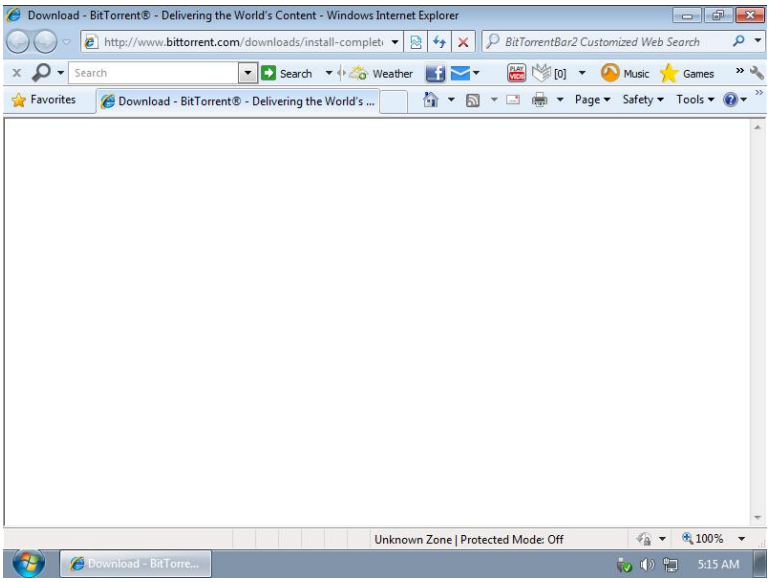

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complet
BitTorrentBar2 Customized Web Search
Search
52°F
[128]
Music
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
BitTorrent
Looking for more?
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
Done, but with errors on page.
Internet | Protected Mode: Off
100%
Download - BitTorre...
5:15 AM

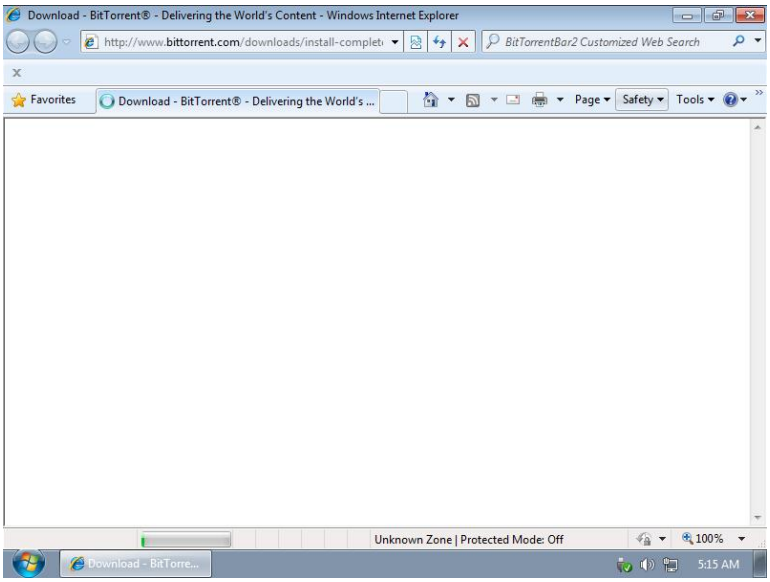

Computer
5:14 AM

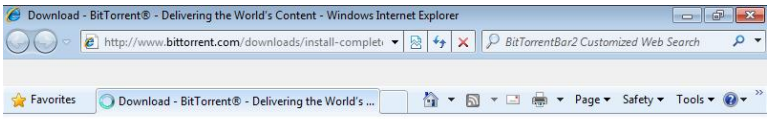

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complet
BitTorrentBar2 Customized Web Search
Search
52°F
[128]
Music
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
BitTorrent
Looking for more?
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
Done, but with errors on page.
Internet | Protected Mode: Off
100%
Download - BitTorre...
You are about to be l...
5:16 AM


Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
BitTorrent
Looking for more?
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
Done, but with errors on page.
Internet | Protected Mode: Off
5:16 AM

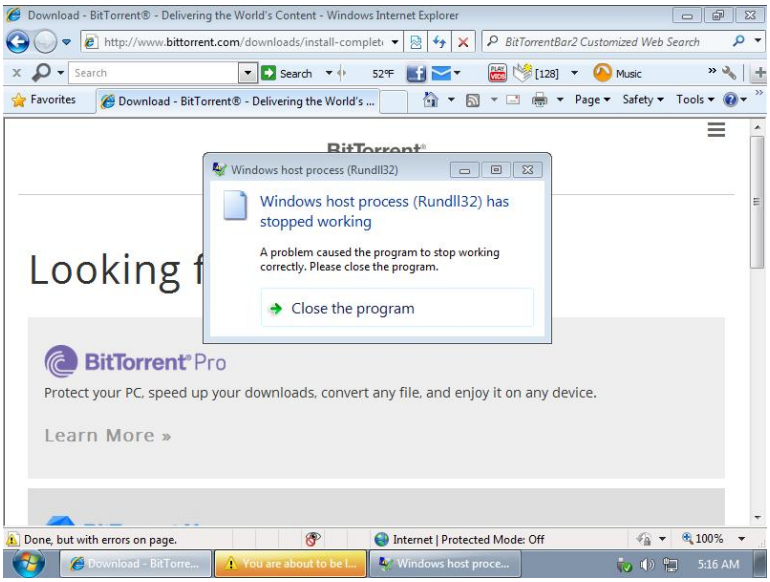

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
BitTorrent
Looking for more?
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
http://www.bittorrent.com/bittorrent-prc
Internet | Protected Mode: Off
5:16 AM

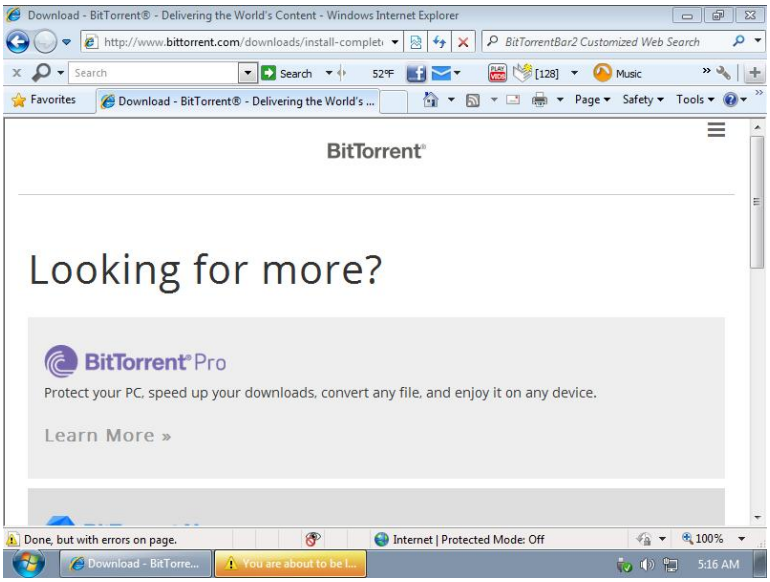

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
Unknown Zone | Protected Mode: Off
5:15 AM

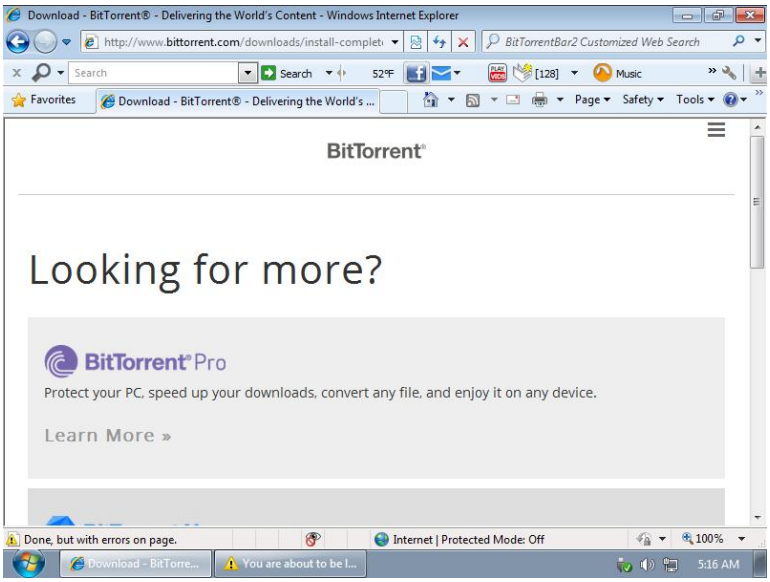

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complet
BitTorrentBar2 Customized Web Search
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
Unknown Zone | Protected Mode: Off
100%
Download - BitTorre...
5:15 AM


Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complet
BitTorrentBar2 Customized Web Search
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools


Download - BitTorre...
5:15 AM


Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complet
BitTorrentBar2 Customized Web Search
Search
52°F
[128]
Music
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
Windows host process (Rundll32)
Windows host process (Rundll32) has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
Looking f
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
Done, but with errors on page.
Internet | Protected Mode: Off
100%
Download - BitTorre...
You are about to be l...
Windows host proce...
5:16 AM


Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complete
BitTorrentBar2 Customized Web Search
Search
52°F
[128]
Music
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
BitTorrent
Looking for more?
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
Done, but with errors on page.
Internet | Protected Mode: Off
100%
Download - BitTorre...
You are about to be l...
5:16 AM

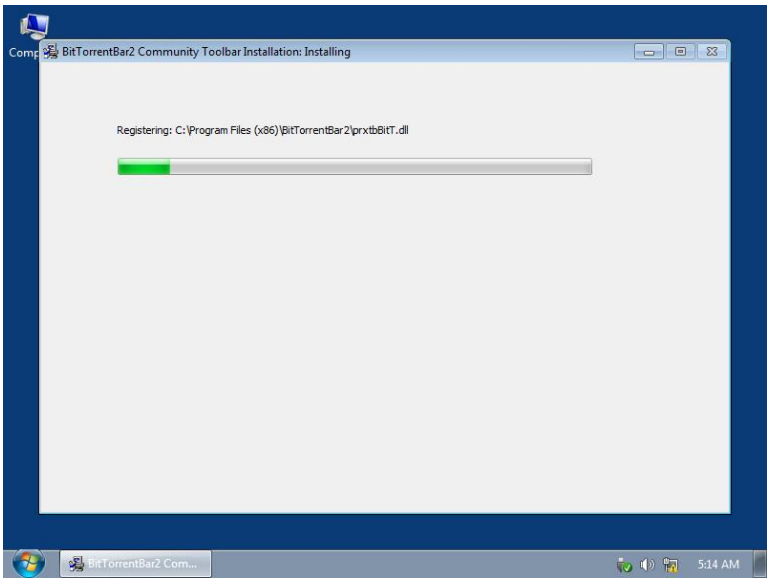

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complete
BitTorrentBar2 Customized Web Search
Search
52°F
[128]
Music
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
BitTorrent
Looking for more?
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
Done, but with errors on page.
Internet | Protected Mode: Off
100%
Download - BitTorre...
You are about to be l...
5:16 AM

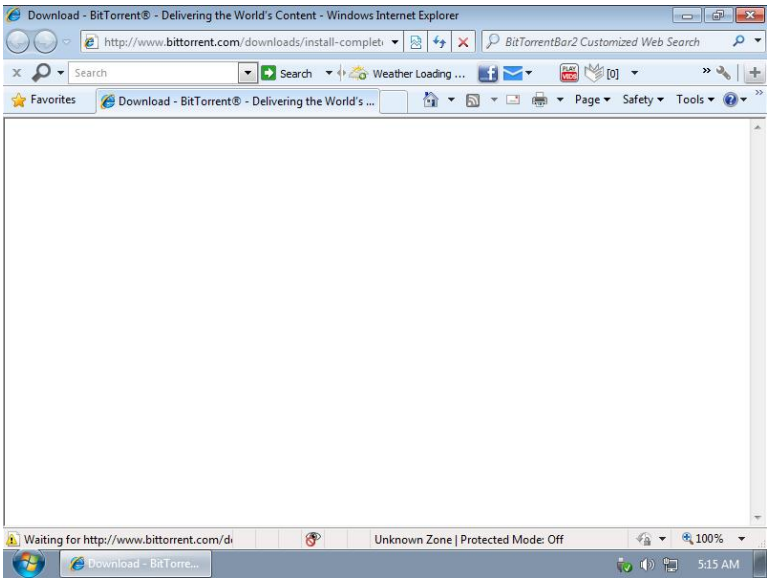

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complete
BitTorrentBar2 Customized Web Search
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools


Unknown Zone | Protected Mode: Off
100%
Download - BitTorre...
5:15 AM


Windows Internet Explorer
Search...
Favorites
Connecting...
Page
Safety
Tools

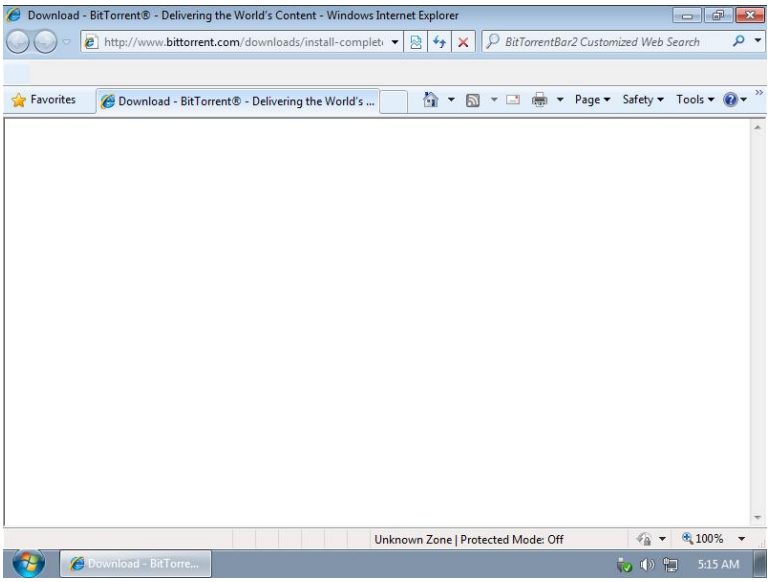

Windows Internet Ex...
5:14 AM

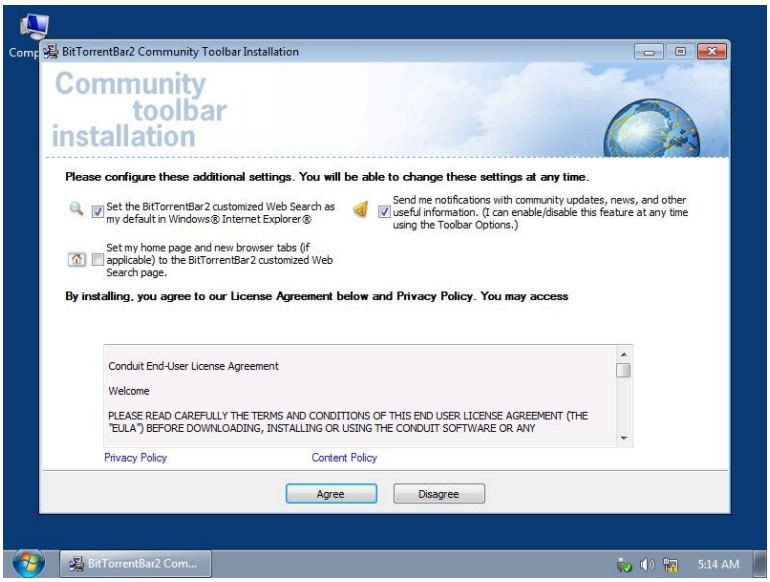

BitTorrentBar2 Community Toolbar Installation: Installing
Registering: C:\Program Files (x86)\BitTorrentBar2\prxtbBitT.dll
BitTorrentBar2 Com...
5:14 AM

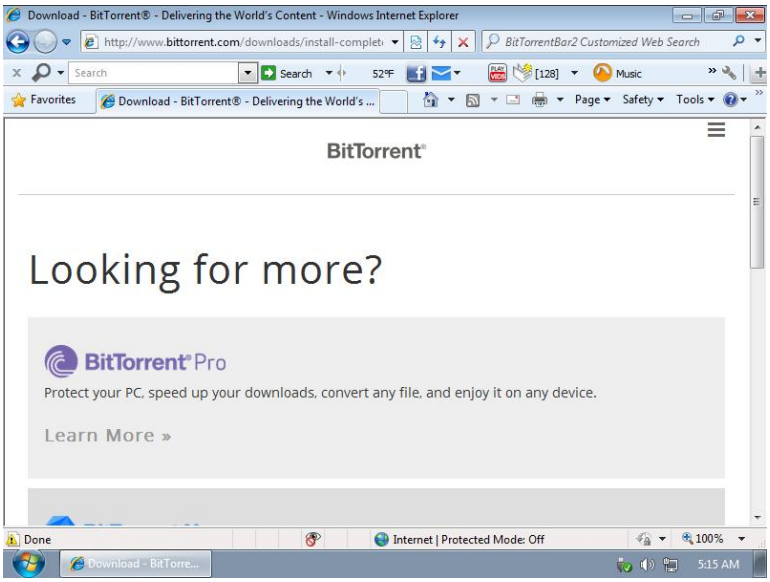

Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complet
BitTorrentBar2 Customized Web Search
Search
Weather Loading ...
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
Waiting for http://www.bittorrent.com/d
Unknown Zone | Protected Mode: Off
100%
Download - BitTorre...
5:15 AM

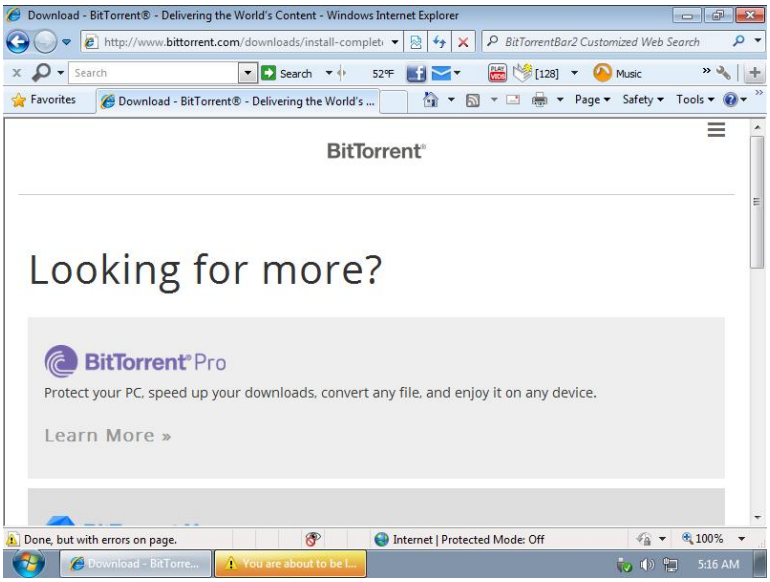

http://www.bittorrent.com/downloads/install-complete - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complete
BitTorrentBar2 Customized Web Search
Favorites
http://www.bittorrent.com/downloads/install-co...
Page
Safety
Tools

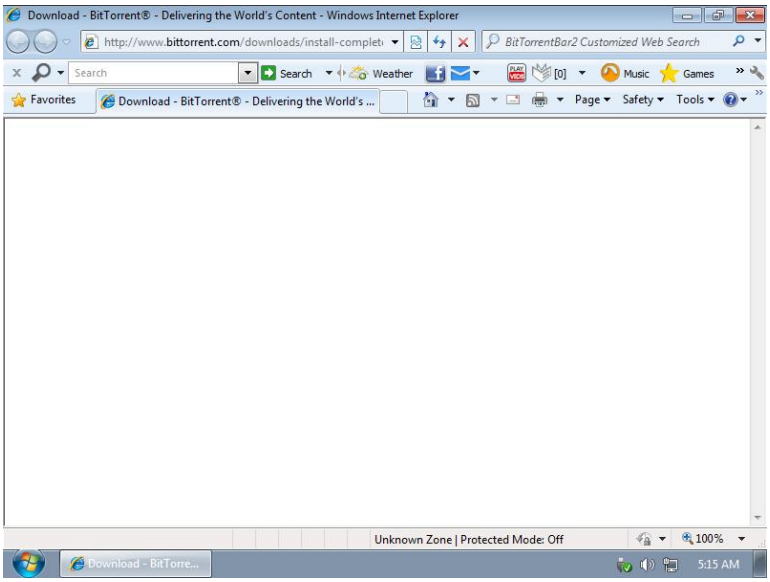

Unknown Zone | Protected Mode: Off
100%
http://www.bittorren...
5:15 AM


Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
http://www.bittorrent.com/downloads/install-complete
BitTorrentBar2 Customized Web Search
Favorites
Download - BitTorrent® - Delivering the World's ...
Page
Safety
Tools
Unknown Zone | Protected Mode: Off
100%
Download - BitTorre...
5:15 AM


BitTorrentBar2 Community Toolbar Installation
Community toolbar installation
Please configure these additional settings. You will be able to change these settings at any time.
Set the BitTorrentBar2 customized Web Search as my default in Windows® Internet Explorer®
Send me notifications with community updates, news, and other useful information. (I can enable/disable this feature at any time using the Toolbar Options.)
Set my home page and new browser tabs (if applicable) to the BitTorrentBar2 customized Web Search page.
By installing, you agree to our License Agreement below and Privacy Policy. You may access
Conduit End-User License Agreement
Welcome
PLEASE READ CAREFULLY THE TERMS AND CONDITIONS OF THIS END USER LICENSE AGREEMENT (THE "EULA") BEFORE DOWNLOADING, INSTALLING OR USING THE CONDUIT SOFTWARE OR ANY
Privacy Policy
Content Policy
Agree
Disagree
BitTorrentBar2 Com...
5:14 AM


Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
BitTorrent
Looking for more?
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
Done
Internet | Protected Mode: Off
5:15 AM


Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
BitTorrent
Looking for more?
BitTorrent Pro
Protect your PC, speed up your downloads, convert any file, and enjoy it on any device.
Learn More »
Done, but with errors on page.
Internet | Protected Mode: Off
5:16 AM


Download - BitTorrent® - Delivering the World's Content - Windows Internet Explorer
Unknown Zone | Protected Mode: Off
5:15 AM