VALKYRIE COMODO

# Summary

**File Name:** None

**File Type:** HTML document, ASCII text, with very long lines

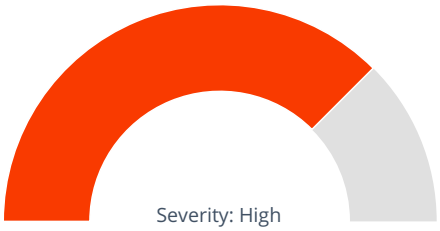
**SHA1:** 849a058cf92f0ae31320d42f3cb06b1585a26386

**MD5:** 122c913d14c61dea54182320cf6ae3a4

MALWARE

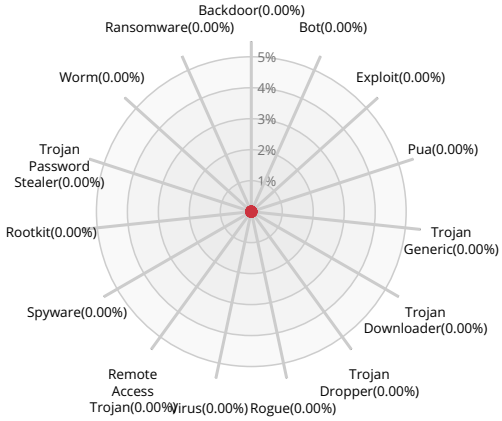
Valkyrie Final Verdict

## DETECTION SECTION

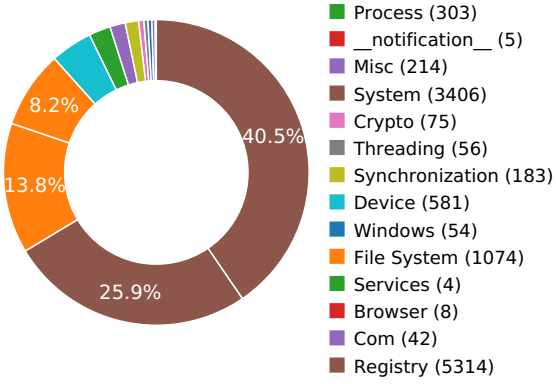



Verdict: Malware

## CLASSIFICATION




## HIGH LEVEL BEHAVIOR DISTRIBUTION




## ACTIVITY OVERVIEW

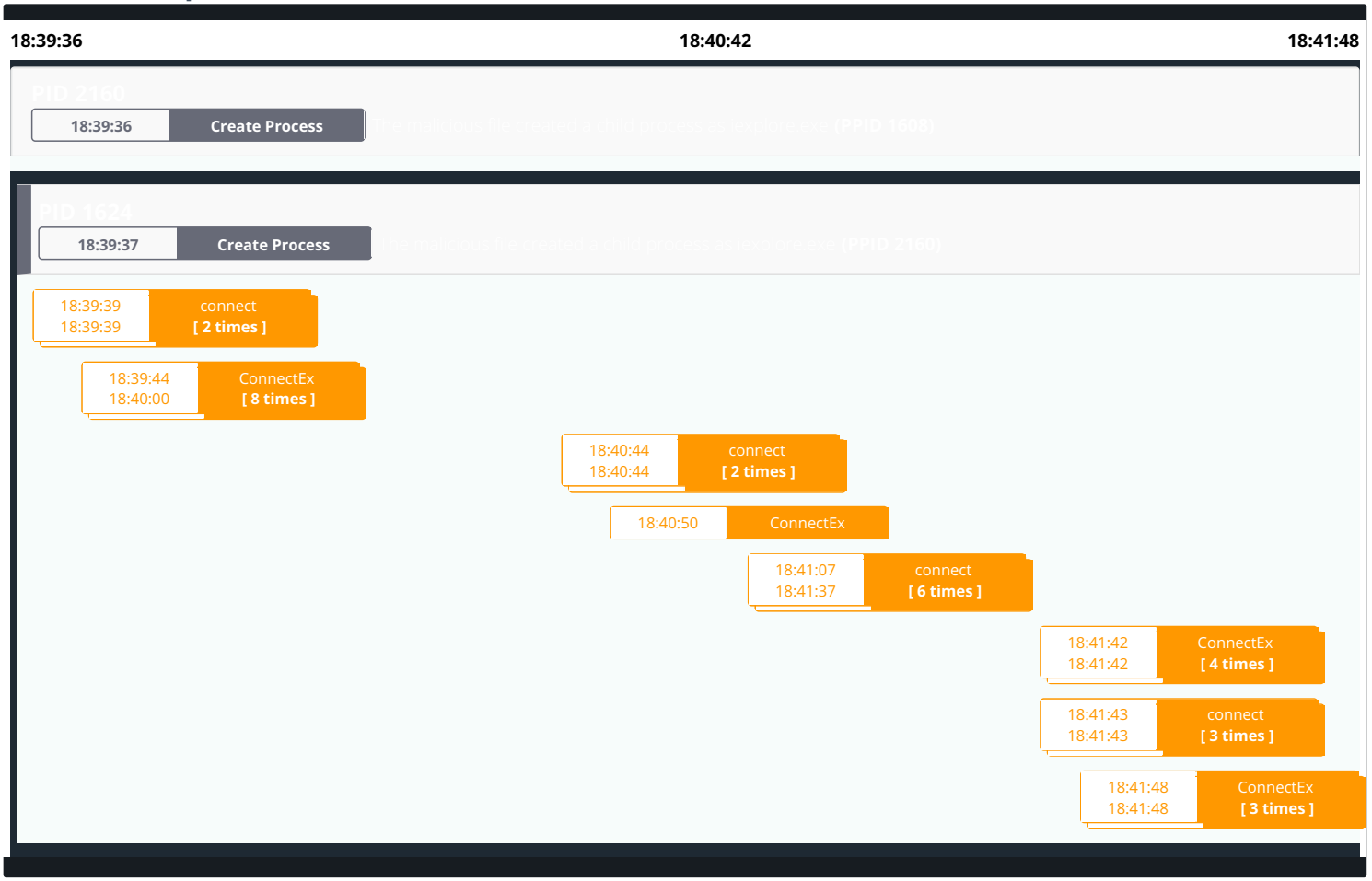
VALKYRIE COMODO

# Activity Details

## NETWORKING

| | |
|---|---|
| Attempts to connect to a dead IP:Port (11 unique times) | Show sources |
| Performs some HTTP requests | Show sources |
| Generates some ICMP traffic | |

## Behavior Graph



VALKYRIE COMODO

## Behavior Summary

### ACCESSED FILES

| |
|---|
| C:\Windows\Globalization\Sorting\sortdefault.nls |
| C:\Program Files (x86)\Internet Explorer\IEShims.dll |
| C:\Windows\SysWOW64\shell32.dll |
| \Device\KsecDD |
| C:\Program Files (x86)\Internet Explorer\sqmapi.dll |
| C:\Users\user\Favorites |
| C:\ |
| C:\Users |
| C:\Users\user\AppData\Local\Microsoft\Windows\Caches |
| 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\user |
| C:\Users\user\Favorites\desktop.ini |
| C:\Users\user\Desktop\desktop.ini |
| \??\MountPointManager |
| C:\Program Files (x86)\Internet Explorer\ieproxy.dll |
| C:\Windows\Fonts\staticcache.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 |
| C:\Program Files (x86)\Common Files\Adobe\Acrobat |
| C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX |
| C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX*.* |
| C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll |
| C:\Windows |
| C:\Windows\winsxs |
| C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll |
| C:\Program Files (x86)\Internet Explorer\iexplore.exe.Local\ |
| C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc |
| C:\Program Files (x86)\Java\jre1.8.0_91\bin\ssv.dll |

| |
|---|
| C:\Program Files (x86)\Java\jre1.8.0_91\bin\ |
| C:\Program Files (x86)\Java |
| C:\Program Files (x86)\Java\jre1.8.0_91\bin |
| C:\Program Files (x86)\Java\jre1.8.0_91\bin*.* |
| C:\Program Files (x86)\Java\jre1.8.0_91\bin\jp2ssv.dll |
| C:\Program Files (x86)\Java\jre1.8.0_91\bin\msvcr100.dll |
| C:\Program Files (x86)\Java\jre1.8.0_91\bin\deploy.dll |
| C:\Program Files (x86)\Java\jre1.8.0_91\lib\plugin.jar |
| C:\Program Files (x86)\Java\jre1.8.0_91\bin\javaws.exe |
| C:\Users\user\AppData\Local\Temp\JavaDeployReg.log |
| C:\Program Files (x86)\Java\jre1.8.0_91 |
| C:\Program Files (x86)\Java\jre1.8.0_91\bin\java.exe |
| C:\Program Files (x86)\Java\jre1.8.0_91\bin\client\jvm.dll |
| C:\Program Files (x86)\Java\jre1.8.0_91\bin\server\jvm.dll |
| C:\Users\user\AppData\Local\Microsoft\Feeds Cache\ |
| C:\Users\user\AppData\Local\Microsoft\Feeds Cache\index.dat |
| C:\Users\user\AppData\Local\Microsoft\Feeds Cache\desktop.ini |
| C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320d42f3cb06b1585a26386.html |
| C:\Users\user\AppData |
| C:\Users\user\AppData\Local |
| C:\Users\user\AppData\Local\Temp |
| C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320d42f3cb06b1585a26386.html:Zone.Identifier |
| C:\Windows\WindowsShell.manifest |
| \??\Nsi |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates* |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342 |

| |
|---|
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\A092A81885DDD5AAD1EC1A803D7183779D81B6F9 |

## READ REGISTRY KEYS

| |
|---|
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\DEPOff |
| HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Low Rights\ProtectedModeOffForAllZones |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\TabProcGrowth |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\TabProcGrowth |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Low Rights\LuaOffLoRIEOn |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FrameTabWindow |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FrameTabWindow |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FrameMerging |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FrameMerging |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\SessionMerging |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\SessionMerging |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\AdminTabProcs |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\AdminTabProcs |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\CompatibilityFlags |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\New Windows\DetourDialogs |
| HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\AcRedir |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US |

| |
|---|
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\RemoteRpcDll |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\TabShutdownDelay |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\TabShutdownDelay |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SQM\ServerFreezeOnUpload |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\Category |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\Name |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\ParentFolder |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\Description |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\RelativePath |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\ParsingName |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\InfoTip |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\LocalizedName |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\Icon |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\Security |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\StreamResource |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\StreamResourceType |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\LocalRedirectOnly |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\Roamable |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\PreCreate |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\Stream |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\PublishExpandedPath |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\Attributes |

| |
|---|
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\FolderTypeID |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\InitFolderHandler |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Favorites |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree |
| HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HasNavigationEnum |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D} |
| 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_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension |

## MODIFIED FILES

| |
|---|
| C:\Users\user\AppData\Local\Temp\JavaDeployReg.log |
| C:\Users\user\AppData\Local\Microsoft\Feeds Cache\index.dat |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 |

| |
|---|
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CFE86DBBE02D859DC92F1E17E0574EE8_FDB452422670E72EDD3FB3D65568F821 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CFE86DBBE02D859DC92F1E17E0574EE8_FDB452422670E72EDD3FB3D65568F821 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F5F320A94D4D2B4465D8F17E2BB2D351_49C072E510849BAED98CE9762AC0F3EF |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F5F320A94D4D2B4465D8F17E2BB2D351_49C072E510849BAED98CE9762AC0F3EF |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\3658603751-ieretrofit[1].js |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\2437439463-css_bundle_v2[1].css |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\authorization[1].css |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F5F320A94D4D2B4465D8F17E2BB2D351_D4C7B7247BFF9536583C1237360C2363 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F5F320A94D4D2B4465D8F17E2BB2D351_D4C7B7247BFF9536583C1237360C2363 |
| C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@google[1].txt |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\plusone[1].js |
| C:\Users\user\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\icon18_wrench_allbkg[1].png |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F5F320A94D4D2B4465D8F17E2BB2D351_7192E4F4CCE38AA73BA653A466481B76 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F5F320A94D4D2B4465D8F17E2BB2D351_7192E4F4CCE38AA73BA653A466481B76 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EDC238BFF48A31D55A97E1E93892934B_C20E0DA2D0F89FE526E1490F4A2EE5AB |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EDC238BFF48A31D55A97E1E93892934B_C20E0DA2D0F89FE526E1490F4A2EE5AB |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\like[1].php |
| C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012018072320180724\index.dat |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\35DDEDF268117918D1D277A171D8DF7B_F2DE72102A14736B534BAAAB62F0BD4B |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\35DDEDF268117918D1D277A171D8DF7B_F2DE72102A14736B534BAAAB62F0BD4B |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\739F2FF4259CDC6CBE7B90F1A95601EF |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\739F2FF4259CDC6CBE7B90F1A95601EF |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\BEC6224B02D155A396218A2504F3EE0B |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\BEC6224B02D155A396218A2504F3EE0B |

## RESOLVED APIS

| |
|---|
| advapi32.dll.EventWrite |
| advapi32.dll.EventRegister |
| advapi32.dll.EventUnregister |
| kernel32.dll.InitializeSRWLock |
| kernel32.dll.AcquireSRWLockExclusive |
| kernel32.dll.AcquireSRWLockShared |
| kernel32.dll.ReleaseSRWLockExclusive |
| kernel32.dll.ReleaseSRWLockShared |

| |
|---|
| kernel32.dll.SetProcessDEPPolicy |
| user32.dll.SetProcessDPIAware |
| shell32.dll.SetCurrentProcessExplicitAppUserModelID |
| user32.dll.GetShellWindow |
| user32.dll.GetWindowThreadProcessId |
| kernel32.dll.SortGetHandle |
| kernel32.dll.SortCloseHandle |
| ieframe.dll.#251 |
| kernel32.dll.WerSetFlags |
| comctl32.dll.PropertySheetW |
| comctl32.dll.PropertySheetA |
| comdlg32.dll.PageSetupDlgW |
| comdlg32.dll.PrintDlgW |
| ieshims.dll.IEShims_Initialize |
| kernel32.dll.VirtualProtect |
| user32.dll.SetWindowsHookExW |
| user32.dll.FindWindowExA |
| kernel32.dll.WaitForSingleObject |
| kernel32.dll.CreateProcessW |
| kernel32.dll.CreateProcessA |
| advapi32.dll.RegQueryValueA |
| ntdll.dll.LdrRegisterDllNotification |
| ole32.dll.CoGetApartmentType |
| ole32.dll.CoTaskMemFree |
| comctl32.dll.#236 |
| oleaut32.dll.#6 |
| ole32.dll.CoTaskMemAlloc |
| ole32.dll.CoGetMalloc |
| cryptbase.dll.SystemFunction036 |
| uxtheme.dll.ThemeInitApiHook |
| user32.dll.IsProcessDPIAware |
| kernel32.dll.WerRegisterMemoryBlock |
| kernel32.dll.WerUnregisterMemoryBlock |
| user32.dll.RegisterWindowMessageW |
| rpcrt4.dll.RpcServerUseProtseqW |

| |
|---|
| rpcrt4.dll.RpcServerRegisterIfEx |
| rpcrtremote.dll.I_RpcExtInitializeExtensionPoint |
| rpcrt4.dll.RpcServerInqBindings |
| rpcrt4.dll.RpcEpRegisterW |
| rpcrt4.dll.RpcServerListen |
| shell32.dll.SHGetInstanceExplorer |
| user32.dll.RegisterClassExW |
| user32.dll.CreateWindowExW |
| user32.dll.DefWindowProcW |
| user32.dll.SetWindowLongW |
| ole32.dll.CoInitializeEx |
| user32.dll.MsgWaitForMultipleObjectsEx |
| dwmapi.dll.DwmIsCompositionEnabled |
| urlmon.dll.#400 |
| shell32.dll.SHGetFolderPathW |
| advapi32.dll.TraceMessage |
| advapi32.dll.TraceMessageVa |
| kernel32.dll.IsWow64Process |
| sqmapi.dll.SqmGetSession |
| sqmapi.dll.SqmEndSession |
| sqmapi.dll.SqmStartSession |
| sqmapi.dll.SqmStartUpload |
| sqmapi.dll.SqmWaitForUploadComplete |
| sqmapi.dll.SqmSet |
| sqmapi.dll.SqmSetBool |
| sqmapi.dll.SqmSetBits |
| sqmapi.dll.SqmSetString |
| sqmapi.dll.SqmIncrement |
| sqmapi.dll.SqmSetIfMax |
| sqmapi.dll.SqmSetIfMin |
| sqmapi.dll.SqmAddToAverage |
| sqmapi.dll.SqmAddToStreamDWord |
| sqmapi.dll.SqmAddToStreamString |

## DELETED FILES

| |
|---|
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\authorization[1].css |
| C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042520160426\index.dat |
| C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042520160426\ |

## REGISTRY KEYS

| |
|---|
| HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\DEPOff |
| HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings |
| HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only |
| HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl |
| HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ENABLESAFESEARCHPATH_KB963027 |
| HKEY_LOCAL_MACHINE\Software\Policies |
| HKEY_CURRENT_USER\Software\Policies |
| HKEY_CURRENT_USER\Software |
| HKEY_LOCAL_MACHINE\Software |
| HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer |
| HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Low Rights |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Low Rights |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Low Rights\ProtectedModeOffForAllZones |
| HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\TabProcGrowth |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\TabProcGrowth |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Low Rights |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Low Rights\LuaOffLoRIEOn |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FrameTabWindow |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FrameTabWindow |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FrameMerging |

| |
|---|
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FrameMerging |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\SessionMerging |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\SessionMerging |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\AdminTabProcs |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\AdminTabProcs |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\CompatibilityFlags |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\New Windows |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\New Windows\DetourDialogs |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\New Windows |
| HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags |
| HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\AcRedir |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon |
| HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US |
| HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\iexplore.exe |
| 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\Policies\Explorer\NoCommonGroups |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Extensions |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\RemoteRpcDll |
| HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BFE |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\TabShutdownDelay |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\TabShutdownDelay |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SQM |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SQM\ServerFreezeOnUpload |

| |
|---|
| HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\SQM |
| HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SQMClient\Windows |
| HKEY_LOCAL_MACHINE\Software\Microsoft\SQMClient\Windows |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD} |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\Category |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\Name |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\ParentFolder |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\Description |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}\RelativePath |

## READ FILES

| |
|---|
| C:\Windows\Globalization\Sorting\sortdefault.nls |
| C:\Program Files (x86)\Internet Explorer\IEShims.dll |
| C:\Windows\SysWOW64\shell32.dll |
| \Device\KsecDD |
| C:\Program Files (x86)\Internet Explorer\sqmapi.dll |
| 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:\Program Files (x86)\Internet Explorer\ieproxy.dll |
| C:\Windows\Fonts\staticcache.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)\Java\jre1.8.0_91\bin\ssv.dll |
| C:\Program Files (x86)\Java\jre1.8.0_91\bin\ |
| C:\Program Files (x86)\Java\jre1.8.0_91\bin\jp2ssv.dll |
| C:\Program Files (x86)\Java\jre1.8.0_91\bin\msvcr100.dll |
| C:\Program Files (x86)\Java\jre1.8.0_91\bin\deploy.dll |
| C:\Users\user\AppData\Local\Temp\JavaDeployReg.log |
| C:\Users\user\AppData\Local\Microsoft\Feeds Cache\index.dat |
| C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320d42f3cb06b1585a26386.html |
| C:\Windows\WindowsShell.manifest |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\A092A81885DDD5AAD1EC1A803D7183779D81B6F9 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\BAED8A8C5A147CFA78E686BB4A8E5829C2F934F5 |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\C8A51E044BF5AF39158BB24E414E8FDCD2891C3A |
| C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\FB45378AB288E369B22C860D123A809F530D5CC1 |
| C:\Windows\System32\en-US\WINHTTP.dll.mui |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 |

| |
|---|
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CFE86DBBE02D859DC92F1E17E0574EE8_FDB452422670E72EDD3FB3D65568F821 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CFE86DBBE02D859DC92F1E17E0574EE8_FDB452422670E72EDD3FB3D65568F821 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F5F320A94D4D2B4465D8F17E2BB2D351_49C072E510849BAED98CE9762AC0F3EF |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F5F320A94D4D2B4465D8F17E2BB2D351_49C072E510849BAED98CE9762AC0F3EF |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\3658603751-ieretrofit[1].js |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\2437439463-css_bundle_v2[1].css |
| C:\Users\user\AppData |
| C:\Users\user\AppData\Local |
| C:\Users\user\AppData\Local\Temp |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\authorization[1].css |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F5F320A94D4D2B4465D8F17E2BB2D351_D4C7B7247BFF9536583C1237360C2363 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F5F320A94D4D2B4465D8F17E2BB2D351_D4C7B7247BFF9536583C1237360C2363 |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\plusone[1].js |
| C:\Users\user\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat |
| C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F5F320A94D4D2B4465D8F17E2BB2D351_7192E4F4CCE38AA73BA653A466481B76 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EDC238BFF48A31D55A97E1E93892934B_C20E0DA2D0F89FE526E1490F4A2EE5AB |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F5F320A94D4D2B4465D8F17E2BB2D351_7192E4F4CCE38AA73BA653A466481B76 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EDC238BFF48A31D55A97E1E93892934B_C20E0DA2D0F89FE526E1490F4A2EE5AB |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\like[1].htm |
| C:\Users\user\AppData\Local\Microsoft |

## MUTEXES

| |
|---|
| Local\WininetStartupMutex |
| Local\c:!users!user!appdata!local!microsoft!feeds cache! |
| Local\ZonesCounterMutex |
| Local\!BrowserEmulation!SharedMemory!Mutex |
| Local\!IETld!Mutex |
| CicLoadWinStaWinSta0 |
| Local\MSCTF.CtfMonitorInstMutexDefault1 |
| IESQMMUTEX_0_208 |
| ConnHashTable<2160>_HashTable_Mutex |
| Local\c:!users!user!appdata!roaming!microsoft!windows!ietldcache! |
| _!SHMSFTHISTORY!_ |

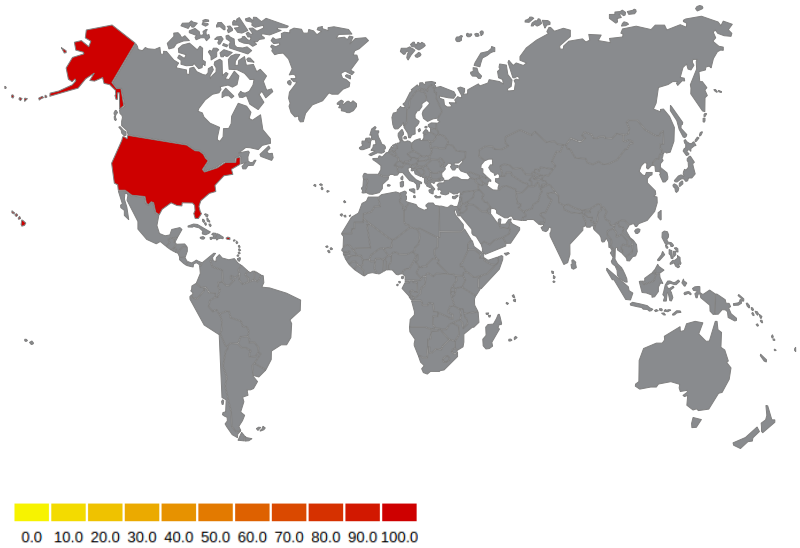
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!mshist012018072320180724!

## MODIFIED REGISTRY KEYS

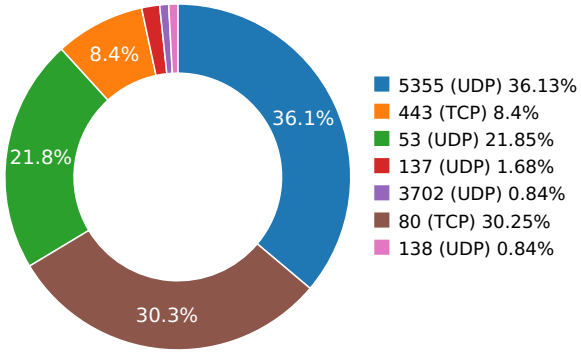
| |
|---|
| HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore\Type |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore\Flags |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore\Count |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore\Time |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore\LoadTime |
| HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore\Type |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore\Flags |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore\Count |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore\Time |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore\LoadTime |
| HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore\Type |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore\Flags |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore\Count |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore\Time |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore\LoadTime |
| HKEY_CLASSES_ROOT\.mhtml\OpenWithList\WINWORD.EXE |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Default MHTML Editor\Last |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012018072320180724 |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012018072320180724\CachePath |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012018072320180724\CachePrefix |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012018072320180724\CacheLimit |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012018072320180724\CacheOptions |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012018072320180724\CacheRepair |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch\Version |

## 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 |
| | 151.101.2.133 | United States | 54113 | Fastly | Malware Process |
| | 184.24.97.176 | United States | 20940 | Akamai Technologies, Inc. | OS Process |
| | 23.215.131.195 | United States | 20940 | Akamai Technologies, Inc. | OS Process |
| | 172.217.7.10 | United States | 15169 | Google LLC | Malware Process |
| | 172.217.6.234 | United States | 15169 | Google LLC | Malware Process |
| | 172.217.6.202 | United States | 15169 | Google LLC | Malware Process |
| | 172.217.3.106 | United States | 15169 | Google LLC | Malware Process |
| | 172.217.12.202 | United States | 15169 | Google LLC | Malware Process |
| | 172.217.12.170 | United States | 15169 | Google LLC | Malware Process |
| | 172.217.12.138 | United States | 15169 | Google LLC | Malware Process |
| | 172.217.11.42 | United States | 15169 | Google LLC | Malware Process |
| | 172.217.11.10 | United States | 15169 | Google LLC | Malware Process |
| | 172.217.10.74 | United States | 15169 | Google LLC | Malware Process |
| | 172.217.10.42 | United States | 15169 | Google LLC | Malware Process |
| | 172.217.10.106 | United States | 15169 | Google LLC | Malware Process |
| | 172.217.10.10 | United States | 15169 | Google LLC | Malware Process |
| | 13.250.71.204 | Singapore | 16509 38895 | Amazon Technologies Inc. | Malware Process |
| crl4.digicert.com | 66.225.197.197 | United States | 30081 | Server Central Network | Malware Process |
| synad2.nuffnang.com.my | 52.221.106.247 | Singapore | 16509 38895 | Amazon Data Services Sing... | Malware Process |
| crl.microsoft.com | 23.215.131.202 | United States | 20940 | Akamai Technologies, Inc. | OS Process |
| 3.bp.blogspot.com | 172.217.10.33 | United States | 15169 | Google LLC | Malware Process |
| lh4.googleusercontent.com | 172.217.10.225 | United States | 15169 | Google LLC | Malware Process |

| Name | IP | Country | ASN | ASN Name | Trigger Process Type |
|---|---|---|---|---|---|
| www.blogger.com | 172.217.10.41 | United States | 15169 | Google LLC | Malware Process |
| www.blogblog.com | 172.217.10.41 | United States | 15169 | Google LLC | Malware Process |
| ctldl.windowsupdate.com | 23.215.131.176 | United States | 20940 | Akamai Technologies, Inc. | OS Process |
| ajax.googleapis.com | 172.217.10.138 | United States | 15169 | Google LLC | Malware Process |
| static.xx.fbcdn.net | 31.13.71.7 | Ireland | 32934 | | Malware Process |
| fonts.gstatic.com | 172.217.10.227 | United States | 15169 | Google LLC | Malware Process |
| ocsp.pki.goog | 172.217.10.46 | United States | 15169 | Google LLC | Malware Process |
| apis.google.com | 172.217.10.238 | United States | 15169 | Google LLC | Malware Process |
| lh6.googleusercontent.com | 172.217.10.225 | United States | 15169 | Google LLC | Malware Process |
| resources.blogblog.com | 172.217.10.41 | United States | 15169 | Google LLC | Malware Process |
| ocsp.digicert.com | 72.21.91.29 | United States | 15133 | MCI Communications Servi... | Malware Process |
| crl.globalsign.net | 104.18.21.226 | United States | 13335 | Cloudflare, Inc. | Malware Process |
| crl3.digicert.com | 72.21.91.29 | United States | 15133 | MCI Communications Servi... | Malware Process |
| www.facebook.com | 31.13.71.38 | Ireland | 32934 | | Malware Process |

## HTTP PACKETS

| Host | Port | Method | Version | User Agent | Count | Call Time During Execution(Sec) |
|---|---|---|---|---|---|---|
| ctldl.windowsupdate.com | 80 | GET | 1.1 | Microsoft-CryptoAPI/6.1 | 1 | 14.1430459023 |
| **Path:** /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8fe89e8d7583f25d<br>**URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?8fe89e8d7583f25d | | | | | | |
| ctldl.windowsupdate.com | 80 | GET | 1.1 | Microsoft-CryptoAPI/6.1 | 1 | 14.1457738876 |
| **Path:** /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?f216704ccf965c53<br>**URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?f216704ccf965c53 | | | | | | |
| ctldl.windowsupdate.com | 80 | GET | 1.1 | Microsoft-CryptoAPI/6.1 | 1 | 19.6584248543 |
| **Path:** /msdownload/update/v3/static/trustedr/en/authrootstl.cab?9581a8356459882f<br>**URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?9581a8356459882f | | | | | | |
| ctldl.windowsupdate.com | 80 | GET | 1.1 | Microsoft-CryptoAPI/6.1 | 1 | 19.65939188 |
| **Path:** /msdownload/update/v3/static/trustedr/en/authrootstl.cab?258904763896e88c<br>**URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?258904763896e88c | | | | | | |
| ocsp.pki.goog | 80 | GET | 1.1 | Microsoft-CryptoAPI/6.1 | 2 | 25.1038339138 |
| **Path:** /gsr2/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBTgXIsxbvr2lBkPpoIEVRE6gHlCnAQUm%2BIHV2ccHsBqBt5ZtJot39wZhi4CDQHjqTAc%2FHIGOD%2BaUx0%3D<br>**URI:** http://ocsp.pki.goog/gsr2/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBTgXIsxbvr2lBkPpoIEVRE6gHlCnAQUm%2BIHV2ccHsBqBt5ZtJot39wZhi4CDQHjqTAc%2FHIGOD%2BaUx0%3D | | | | | | |
| ocsp.pki.goog | 80 | GET | 1.1 | Microsoft-CryptoAPI/6.1 | 2 | 30.3267390728 |
| **Path:** /GTSGIAG3/MEkwRzBFMEMwQTAJBgUrDgMCGgUABBT27bBjYjKBmjX2jXWgnQJKEapsrQQUd8K4UJpndnaxLcKG0IOgfqZ%2BuksCCFA3qWe6x%2F05<br>**URI:** http://ocsp.pki.goog/GTSGIAG3/MEkwRzBFMEMwQTAJBgUrDgMCGgUABBT27bBjYjKBmjX2jXWgnQJKEapsrQQUd8K4UJpndnaxLcKG0IOgfqZ%2BuksCCFA3qWe6x%2F05 | | | | | | |

| Host | Port | Method | Version | User Agent | Count | Call Time During Execution(Sec) |
|---|---|---|---|---|---|---|
| crl.microsoft.com | 80 | GET | 1.1 | Microsoft-CryptoAPI/6.1 | 1 | 65.8777248859 |
| **Path:** /pki/crl/products/tspca.crl<br>**URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl | | | | | | |
| crl.microsoft.com | 80 | GET | 1.1 | Microsoft-CryptoAPI/6.1 | 1 | 71.0180740356 |
| **Path:** /pki/crl/products/CodeSignPCA2.crl<br>**URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl | | | | | | |
| crl.microsoft.com | 80 | GET | 1.1 | Microsoft-CryptoAPI/6.1 | 1 | 76.1574790478 |
| **Path:** /pki/crl/products/WinPCA.crl<br>**URI:** http://crl.microsoft.com/pki/crl/products/WinPCA.crl | | | | | | |
| ocsp.pki.goog | 80 | GET | 1.1 | Microsoft-CryptoAPI/6.1 | 1 | 79.483301878 |
| **Path:** /GTSGIAG3/MEkwRzBFMEMwQTAJBgUrDgMCGgUABBT27bBjYjKBmjX2jXWgnQJKEapsrQQUd8K4UJpndnaxLcKG0IOgfqZ%2BuksCCE%2F4f4kx%2B79J<br>**URI:** http://ocsp.pki.goog/GTSGIAG3/MEkwRzBFMEMwQTAJBgUrDgMCGgUABBT27bBjYjKBmjX2jXWgnQJKEapsrQQUd8K4UJpndnaxLcKG0IOgfqZ%2BuksCCE%2F4f4kx%2B79J | | | | | | |
| crl.globalsign.net | 80 | GET | 1.1 | Microsoft-CryptoAPI/6.1 | 1 | 81.347591877 |
| **Path:** /primobject.crl<br>**URI:** http://crl.globalsign.net/primobject.crl | | | | | | |
| www.facebook.com | 80 | GET | 1.1 | Mozilla/4.0 (compatible; MS... | 1 | 127.118281841 |
| **Path:** /plugins/like.php?href=www.facebook.com/pages/Khaiza-Mom-Store/600334830027619&layout=button_count&show_faces=false&width=50&action=like&colorscheme=light&height=21<br>**URI:** http://www.facebook.com/plugins/like.php?href=www.facebook.com/pages/Khaiza-Mom-Store/600334830027619&layout=button_count&show_faces=false&width=50&action=like&colorscheme=light&height=21 | | | | | | |
| ocsp.pki.goog | 80 | GET | 1.1 | Microsoft-CryptoAPI/6.1 | 3 | 132.201676846 |
| **Path:** /GTSGIAG3/MEkwRzBFMEMwQTAJBgUrDgMCGgUABBT27bBjYjKBmjX2jXWgnQJKEapsrQQUd8K4UJpndnaxLcKG0IOgfqZ%2BuksCCEM5Rm4ycYDk<br>**URI:** http://ocsp.pki.goog/GTSGIAG3/MEkwRzBFMEMwQTAJBgUrDgMCGgUABBT27bBjYjKBmjX2jXWgnQJKEapsrQQUd8K4UJpndnaxLcKG0IOgfqZ%2BuksCCEM5Rm4ycYDk | | | | | | |
| ocsp.digicert.com | 80 | GET | 1.1 | Microsoft-CryptoAPI/6.1 | 1 | 132.398280859 |
| **Path:** /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCzkdAQpVYowQUsT7DaQP4v0cB1JgmGggC72NkK8MCEATh56TcXPLzbcArQrhdFZ8%3D<br>**URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCzkdAQpVYowQUsT7DaQP4v0cB1JgmGggC72NkK8MCEATh56TcXPLzbcArQrhdFZ8%3D | | | | | | |
| ocsp.digicert.com | 80 | GET | 1.1 | Microsoft-CryptoAPI/6.1 | 1 | 137.577550888 |
| **Path:** /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTPJvUY%2Bsl%2Bj4yzQuAcL2oQno5fCgQUUWj%2FkK8CB3U8zNllZGKiErhZcjsCEAs8O2AaGPWe4ra7BWBe8sA%3D<br>**URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTPJvUY%2Bsl%2Bj4yzQuAcL2oQno5fCgQUUWj%2FkK8CB3U8zNllZGKiErhZcjsCEAs8O2AaGPWe4ra7BWBe8sA%3D | | | | | | |
| crl4.digicert.com | 80 | GET | 1.1 | Microsoft-CryptoAPI/6.1 | 1 | 137.673243046 |
| **Path:** /sha2-ha-server-g6.crl<br>**URI:** http://crl4.digicert.com/sha2-ha-server-g6.crl | | | | | | |
| crl3.digicert.com | 80 | GET | 1.1 | Microsoft-CryptoAPI/6.1 | 1 | 137.693019867 |
| **Path:** /sha2-ha-server-g6.crl<br>**URI:** http://crl3.digicert.com/sha2-ha-server-g6.crl | | | | | | |

## DNS QUERIES

| Request | Type |
|---|---|
| www.blogger.com | A |
| **Answers**<br>- 172.217.10.41 (A)<br>- blogger.l.google.com (CNAME) | |
| ctldl.windowsupdate.com | A |
| **Answers**<br>- ctldl.windowsupdate.nsatc.net (CNAME)<br>- 184.24.97.176 (A)<br>- a1621.g.akamai.net (CNAME)<br>- ctldl.windowsupdate.com.edgesuite.net (CNAME)<br>- 184.24.97.174 (A)<br>- 23.215.131.176 (A)<br>- 23.215.131.169 (A) | |
| ocsp.pki.goog | A |
| **Answers**<br>- www3.l.google.com (CNAME)<br>- 172.217.10.46 (A) | |
| ajax.googleapis.com | A |
| **Answers**<br>- 172.217.12.138 (A)<br>- 172.217.10.106 (A)<br>- 172.217.12.170 (A)<br>- 172.217.11.10 (A)<br>- googleapis.l.google.com (CNAME)<br>- 172.217.10.74 (A)<br>- 172.217.10.42 (A)<br>- 172.217.12.202 (A)<br>- 172.217.11.42 (A)<br>- 172.217.3.106 (A)<br>- 172.217.7.10 (A)<br>- 172.217.10.10 (A)<br>- 172.217.6.234 (A)<br>- 172.217.6.202 (A)<br>- 172.217.10.138 (A)<br>- 172.217.10.234 (A) | |
| fonts.gstatic.com | A |
| **Answers**<br>- 172.217.10.227 (A)<br>- gstaticadssl.l.google.com (CNAME) | |
| crl.microsoft.com | A |
| **Answers**<br>- crl.www.ms.akadns.net (CNAME)<br>- 23.215.131.200 (A)<br>- 23.215.131.195 (A)<br>- a1363.dscg.akamai.net (CNAME) | |
| apis.google.com | A |
| **Answers**<br>- 172.217.10.238 (A)<br>- plus.l.google.com (CNAME) | |
| 3.bp.blogspot.com | A |

| Request | Type |
|---|---|
| **Answers**<br>- photos-ugc.l.googleusercontent.com (CNAME)<br>- 172.217.10.33 (A) | |
| www.blogblog.com | A |
| crl.globalsign.net | A |
| **Answers**<br>- 151.101.66.133 (A)<br>- 151.101.2.133 (A)<br>- global.prd.cdn.globalsign.com (CNAME)<br>- 151.101.194.133 (A)<br>- 151.101.130.133 (A)<br>- prod.globalsign.map.fastly.net (CNAME) | |
| resources.blogblog.com | A |
| synad2.nuffnang.com.my | A |
| **Answers**<br>- 13.250.71.204 (A)<br>- nuffnang.com.my (CNAME)<br>- 52.221.106.247 (A) | |
| lh6.googleusercontent.com | A |
| lh4.googleusercontent.com | A |
| **Answers**<br>- googlehosted.l.googleusercontent.com (CNAME)<br>- 172.217.10.225 (A) | |
| www.facebook.com | A |
| **Answers**<br>- star-z-mini.c10r.facebook.com (CNAME)<br>- 31.13.71.38 (A) | |
| ocsp.digicert.com | A |
| **Answers**<br>- cs9.wac.phicdn.net (CNAME)<br>- 72.21.91.29 (A) | |
| static.xx.fbcdn.net | A |
| **Answers**<br>- 31.13.71.7 (A)<br>- scontent.xx.fbcdn.net (CNAME) | |
| crl3.digicert.com | A |
| crl4.digicert.com | A |
| **Answers**<br>- digicert.cachefly.net (CNAME)<br>- 66.225.197.197 (A)<br>- rvip1.ue.cachefly.net (CNAME) | |

## TCP PACKETS

| Call Time During Execution(sec) | Source IP | Dest IP | Dest Port |
|---|---|---|---|
| 8.4699678421 | Sandbox | 172.217.10.41 | 443 |
| 8.470733881 | Sandbox | 172.217.10.41 | 443 |
| 14.1430459023 | Sandbox | 23.215.131.176 | 80 |
| 14.1457738876 | Sandbox | 184.24.97.176 | 80 |
| 19.6584248543 | Sandbox | 184.24.97.176 | 80 |
| 19.65939188 | Sandbox | 184.24.97.176 | 80 |
| 25.1038339138 | Sandbox | 172.217.10.46 | 80 |
| 25.1047949791 | Sandbox | 172.217.10.46 | 80 |
| 30.3267390728 | Sandbox | 172.217.10.46 | 80 |
| 30.3279709816 | Sandbox | 172.217.10.46 | 80 |
| 65.8777248859 | Sandbox | 23.215.131.195 | 80 |
| 74.0529539585 | Sandbox | 172.217.10.41 | 443 |
| 74.2678370476 | Sandbox | 172.217.10.238 | 443 |
| 79.483301878 | Sandbox | 172.217.10.46 | 80 |
| 81.347591877 | Sandbox | 151.101.2.133 | 80 |
| 96.5499930382 | Sandbox | 172.217.10.41 | 443 |
| 126.792180061 | Sandbox | 172.217.10.225 | 443 |
| 126.793241978 | Sandbox | 172.217.10.225 | 443 |
| 126.793736935 | Sandbox | 172.217.10.225 | 443 |
| 127.118281841 | Sandbox | 31.13.71.38 | 80 |
| 127.174017906 | Sandbox | 31.13.71.38 | 443 |
| 132.201676846 | Sandbox | 172.217.10.46 | 80 |
| 132.20215106 | Sandbox | 172.217.10.46 | 80 |
| 132.202760935 | Sandbox | 172.217.10.46 | 80 |
| 132.398280859 | Sandbox | 72.21.91.29 | 80 |
| 132.487732887 | Sandbox | 31.13.71.38 | 443 |
| 137.577550888 | Sandbox | 72.21.91.29 | 80 |
| 137.673243046 | Sandbox | 66.225.197.197 | 80 |
| 137.693019867 | Sandbox | 72.21.91.29 | 80 |

## UDP PACKETS

| Call Time During Execution(sec) | Source IP | Dest IP | Dest Port |
|---|---|---|---|
| 3.129997015 | Sandbox | 224.0.0.252 | 5355 |
| 3.19416093826 | Sandbox | 192.168.56.255 | 137 |
| 3.21350097656 | Sandbox | 224.0.0.252 | 5355 |

| Call Time During Execution(sec) | Source IP | Dest IP | Dest Port |
|---|---|---|---|
| 3.25540304184 | Sandbox | 239.255.255.250 | 3702 |
| 5.76939606667 | Sandbox | 224.0.0.252 | 5355 |
| 8.39447689056 | Sandbox | 8.8.4.4 | 53 |
| 8.82902598381 | Sandbox | 224.0.0.252 | 5355 |
| 8.83167290688 | Sandbox | 224.0.0.252 | 5355 |
| 9.18877696991 | Sandbox | 192.168.56.255 | 138 |
| 11.4506819248 | Sandbox | 224.0.0.252 | 5355 |
| 11.4509940147 | Sandbox | 224.0.0.252 | 5355 |
| 14.0050508976 | Sandbox | 8.8.4.4 | 53 |
| 14.0054719448 | Sandbox | 8.8.4.4 | 53 |
| 14.494343996 | Sandbox | 224.0.0.252 | 5355 |
| 14.4963409901 | Sandbox | 224.0.0.252 | 5355 |
| 17.0735628605 | Sandbox | 224.0.0.252 | 5355 |
| 17.0738918781 | Sandbox | 224.0.0.252 | 5355 |
| 19.9047548771 | Sandbox | 224.0.0.252 | 5355 |
| 19.9050879478 | Sandbox | 224.0.0.252 | 5355 |
| 22.5118079185 | Sandbox | 224.0.0.252 | 5355 |
| 22.5121798515 | Sandbox | 224.0.0.252 | 5355 |
| 25.0648598671 | Sandbox | 8.8.4.4 | 53 |
| 25.0652689934 | Sandbox | 8.8.4.4 | 53 |
| 25.1808290482 | Sandbox | 224.0.0.252 | 5355 |
| 25.1816029549 | Sandbox | 224.0.0.252 | 5355 |
| 27.7613520622 | Sandbox | 224.0.0.252 | 5355 |
| 27.7616689205 | Sandbox | 224.0.0.252 | 5355 |
| 30.7791650295 | Sandbox | 8.8.4.4 | 53 |
| 30.7925879955 | Sandbox | 8.8.4.4 | 53 |
| 31.9085998535 | Sandbox | 8.8.4.4 | 53 |
| 52.9135110378 | Sandbox | 8.8.4.4 | 53 |
| 60.6616079807 | Sandbox | 224.0.0.252 | 5355 |
| 63.2494699955 | Sandbox | 224.0.0.252 | 5355 |
| 65.8036940098 | Sandbox | 8.8.4.4 | 53 |
| 65.9059178829 | Sandbox | 224.0.0.252 | 5355 |
| 68.4633820057 | Sandbox | 224.0.0.252 | 5355 |
| 71.045003891 | Sandbox | 224.0.0.252 | 5355 |
| 73.6048910618 | Sandbox | 224.0.0.252 | 5355 |
| 74.2280359268 | Sandbox | 8.8.4.4 | 53 |
| 74.2644579411 | Sandbox | 8.8.4.4 | 53 |

| Call Time During Execution(sec) | Source IP | Dest IP | Dest Port |
|---|---|---|---|
| 74.2686860561 | Sandbox | 8.8.4.4 | 53 |
| 74.3508708477 | Sandbox | 224.0.0.252 | 5355 |
| 75.424448967 | Sandbox | 8.8.4.4 | 53 |
| 76.1798009872 | Sandbox | 224.0.0.252 | 5355 |
| 76.9221098423 | Sandbox | 224.0.0.252 | 5355 |
| 77.6729750633 | Sandbox | 8.8.4.4 | 53 |
| 77.7952780724 | Sandbox | 172.217.10.41 | 137 |
| 78.7449698448 | Sandbox | 224.0.0.252 | 5355 |
| 81.3019390106 | Sandbox | 8.8.4.4 | 53 |
| 96.5043408871 | Sandbox | 8.8.4.4 | 53 |
| 96.5446379185 | Sandbox | 8.8.4.4 | 53 |
| 97.6917369366 | Sandbox | 8.8.4.4 | 53 |
| 126.75012207 | Sandbox | 8.8.4.4 | 53 |
| 126.750644922 | Sandbox | 8.8.4.4 | 53 |
| 127.025928974 | Sandbox | 8.8.4.4 | 53 |
| 127.033630848 | Sandbox | 224.0.0.252 | 5355 |
| 127.03768301 | Sandbox | 224.0.0.252 | 5355 |
| 127.039941072 | Sandbox | 224.0.0.252 | 5355 |
| 127.235889912 | Sandbox | 224.0.0.252 | 5355 |
| 129.630646944 | Sandbox | 224.0.0.252 | 5355 |
| 129.631104946 | Sandbox | 224.0.0.252 | 5355 |
| 129.63150692 | Sandbox | 224.0.0.252 | 5355 |
| 129.81454587 | Sandbox | 224.0.0.252 | 5355 |
| 132.376680851 | Sandbox | 8.8.4.4 | 53 |
| 132.443130016 | Sandbox | 224.0.0.252 | 5355 |
| 132.45756197 | Sandbox | 224.0.0.252 | 5355 |
| 132.471997976 | Sandbox | 224.0.0.252 | 5355 |
| 132.763648987 | Sandbox | 8.8.4.4 | 53 |
| 135.014338017 | Sandbox | 224.0.0.252 | 5355 |
| 135.027189016 | Sandbox | 224.0.0.252 | 5355 |
| 135.05094099 | Sandbox | 224.0.0.252 | 5355 |
| 137.579253912 | Sandbox | 8.8.4.4 | 53 |
| 137.610532045 | Sandbox | 8.8.4.4 | 53 |

VALKYRIE COMODO

DETAILED FILE INFO

## CREATED / DROPPED FILES

| FILE PATH | TYPE AND HASHES |
|---|---|
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\35DDEDF268117918D1D277A171D8DF7B_F2DE72102A14736B534BAAAB62F0BD4B** | **Type :** data<br>**MD5 :** ae8dbeaada58b02660374c68bbea5173<br>**SHA-1 :** 9a33695f46944998382d196b3445ecd588444d16<br>**SHA-256 :** fae1aace511ce717a6893376903163511d362872<br>**SHA-512 :** c3dd1b070ef30efee4f68e9efaad346cf83948d23<br>**Size :** 0.471 Kilobytes. |
| **C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\Icon18_wrench_allbkg[1].Png** | **Type :** PNG image data, 18 x 18, 8-bit colormap, non-interlaced<br>**MD5 :** f617effe6d96c15acfea8b2e8aae551f<br>**SHA-1 :** 6d676af11ad2e84b620cce4d5992b657cb2d8ab6<br>**SHA-256 :** d172d750493be64a7ed84dec1dd2a0d787ba42f<br>**SHA-512 :** 3189a6281ad065848afc700a47bea885cd3905da<br>**Size :** 0.475 Kilobytes. |
| **C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\Index.Dat** | **Type :** Internet Explorer cache file version Ver 5.2<br>**MD5 :** 55822ceacafb8f75b9c68f8b803f37e3<br>**SHA-1 :** 95fc79bb8ad504e06d80a7dd9648badd7d0ccc0d<br>**SHA-256 :** 3b2057438c3f47591e8f6824d2dea3eaef59e7a7a<br>**SHA-512 :** 1a498862b2f740d80fed4758cff4fb20fb61da06fb<br>**Size :** 32.768 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\35DDEDF268117918D1D277A171D8DF7B_F2DE72102A14736B534BAAAB62F0BD4B** | **Type :** data<br>**MD5 :** 31c55fb5ec971cd8709dea922e5dc16a<br>**SHA-1 :** 5074c22c6137ed8eecdecc3ba0084062ac0a1487<br>**SHA-256 :** 6b97cb9b1815bb4649c7f6e233b3f86ec4c0838c<br>**SHA-512 :** 88a27e255f397581f91aee1f78b0d4f8b36be425b<br>**Size :** 0.438 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157** | **Type :** Microsoft Cabinet archive data, 6509 bytes, 1 file<br>**MD5 :** 33b39e2a516ef730a8fa922894f0fbd5<br>**SHA-1 :** 03d455583dda59215d945af76af6293b202f586f<br>**SHA-256 :** 9446e8f2056fea3ac1365a809ada04602606242c<br>**SHA-512 :** 75763aa13b43eb96294b0f84e13106611198872<br>**Size :** 6.509 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506** | **Type :** Microsoft Cabinet archive data, 54062 bytes, 1 file<br>**MD5 :** 46ba6cf8c185742795687a489238da0b<br>**SHA-1 :** a0caf545a4ea1694a62c38617f2902e07803326f<br>**SHA-256 :** 80bd068ab6e55ee508fda18c7ae8507d7fbd6a28<br>**SHA-512 :** 8b518f4f2126c7a67823fe74b17a1078b42cfb59e<br>**Size :** 54.062 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506** | **Type :** data<br>**MD5 :** 0d3c93a96e9eff37446d139a43f12ff8<br>**SHA-1 :** 35170f80eff17b0eaa4ec8414aa6038c3a4941e6<br>**SHA-256 :** 72d1d632a85c562aeeb9d65ced15cc8d7ac0d103<br>**SHA-512 :** cbf9257a612d7d548467d0720dbc42c4fc5bdbe7<br>**Size :** 0.326 Kilobytes. |
| **C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\2437439463-Css_bundle_v2[1].Css** | **Type :** ASCII text, with very long lines<br>**MD5 :** a9a2edaa7626c4ea076544025a965aaf<br>**SHA-1 :** b6eac9f7509c55c0f4718b2948e56fe7127f05c8<br>**SHA-256 :** 9ab222347578ca0ec423daad8b0e694c643f5180<br>**SHA-512 :** 906b9471e9188e8cfc362c0e1d8a4d83ce782d72<br>**Size :** 41.572 Kilobytes. |

| FILE PATH | TYPE AND HASHES |
|---|---|
| **C:\Users\User\AppData\Local\Microsoft\Feeds Cache\Index.Dat** | **Type :** Internet Explorer cache file version Ver 5.2<br>**MD5 :** 3e5ddabe53f537bb917138b79e28e6e7<br>**SHA-1 :** 7dac8bae102d9252a0c912a4ff6a42295ec1e8fe<br>**SHA-256 :** 921a68e66c33e22dba1677e4a0a7a1367c54108<br>**SHA-512 :** eecbc6736703384c56642f4fa602e8a8673ed70f6<br>**Size :** 32.768 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F5F320A94D4D2B4465D8F17E2BB2D351_49C072E510849BAED98CE9762AC0F3EF** | **Type :** data<br>**MD5 :** b56b844a1a6c5ec7fdad32e1672ded2f<br>**SHA-1 :** c864e86f97d52a096f80226cdfd5bceeb0ea6822<br>**SHA-256 :** 7c3d6ab30a71bac881c48457a4ba4d5f4e18f2be<br>**SHA-512 :** 4053833d8e19bc8e4b0511b53ce7520c1560eb9<br>**Size :** 0.386 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F5F320A94D4D2B4465D8F17E2BB2D351_7192E4F4CCE38AA73BA653A466481B76** | **Type :** data<br>**MD5 :** 88d50e3a8087b828be4194045415520f<br>**SHA-1 :** cf866b269233039dd17e11d107cc759eb224e2fb<br>**SHA-256 :** 2996547ae0bc160d23b6dfa92a61b3883d90758<br>**SHA-512 :** bc0ab5e6bae3e33385f75d77f78ecc61ecc5e2ca0<br>**Size :** 0.382 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157** | **Type :** data<br>**MD5 :** 39cb763853c0504756116b720c1e3f17<br>**SHA-1 :** e3bec5e14495c01e83b149743dcae6b0e4cde7ef<br>**SHA-256 :** 8510c196a2186de7c3a9a4506e3ba9a3716be7fe<br>**SHA-512 :** d085a332ad30a0780f5caa83176faa954f77e391<br>**Size :** 0.342 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\739F2FF4259CDC6CBE7B90F1A95601EF**<br>**C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\BEC6224B02D155A396218A2504F3EE0B** | **Type :** data<br>**MD5 :** 943b75b5b8c5e0f020bcc3f6362c7266<br>**SHA-1 :** 64e0eb2d27ff05e62c4a369a59f1dcd6524b5702<br>**SHA-256 :** 6ba6886140c43d5c6d51d56380e58ac9347a8e9<br>**SHA-512 :** f273b5cd0d28bf223409c7714d7938c8764e529a<br>**Size :** 105.184 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CFE86DBBE02D859DC92F1E17E0574EE8_FDB452422670E72EDD3FB3D65568F821** | **Type :** data<br>**MD5 :** 26cf9296ef9e1e45cd2884df57da2e86<br>**SHA-1 :** 9e4821b13c8f0257c3f1f45c175733a4db80b8e8<br>**SHA-256 :** 0fffeddb6d92ed003d857fd67a24e278b6301a49<br>**SHA-512 :** e9592b1e0ff706a0b8e0363226e2b6ccf6ca2cc32<br>**Size :** 0.402 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F5F320A94D4D2B4465D8F17E2BB2D351_D4C7B7247BFF9536583C1237360C2363** | **Type :** data<br>**MD5 :** afa936edbbb7bec95839f6bf0e31a7a3<br>**SHA-1 :** 1f6a7324876c2d5228091e9a8ff76e7a11e7dea4<br>**SHA-256 :** 18d10ce2b557d900ef1cfac08059beaca9e5d25d<br>**SHA-512 :** 23d1b793326bdf9d8e408e87e4bff555f585fe8c7<br>**Size :** 0.39 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\739F2FF4259CDC6CBE7B90F1A95601EF** | **Type :** data<br>**MD5 :** 8885a4e897fa2a0035e5f514bef84685<br>**SHA-1 :** bf2582fd7224fa2fa69eb31604304afb743e1119<br>**SHA-256 :** e8240414ec04abf6c0097cc1b1d925ee4b056fd1<br>**SHA-512 :** 4b0149ccc1869f404feda39d937003037a73a320<br>**Size :** 0.21 Kilobytes. |
| **C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\Plusone[1].Js** | **Type :** ASCII text, with very long lines<br>**MD5 :** d618491de99a38ec88bd084bb3b99af3<br>**SHA-1 :** acbd1db6b9c09e765d90f9c57ea205482366654d<br>**SHA-256 :** 2c51f3d925292ba6aab0bbc4c4c4c9983a21dd23<br>**SHA-512 :** 2e59d5c18c1737abf36c837024d2f8d10ca0b25b<br>**Size :** 44.024 Kilobytes. |

| FILE PATH | TYPE AND HASHES |
|---|---|
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F5F320A94D4D2B4465D8F17E2BB2D351_7192E4F4CCE38AA73BA653A466481B76** | **Type :** data<br>**MD5 :** 75c55c1dd3142a28bd4f0a4501b9ff15<br>**SHA-1 :** d39ce0b0be1f08685f0fdb54eb4420e6c0c425b5<br>**SHA-256 :** ada89de06960ce6e5700b19f1c9faa76b6698cd1<br>**SHA-512 :** 463f2cde990439f417891f0b24c28f26c9d751bbd<br>**Size :** 0.463 Kilobytes. |
| **C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@Google[1].Txt** | **Type :** ASCII text<br>**MD5 :** 8217aba7a1d3112bb145d90eca17152b<br>**SHA-1 :** 0d80d145b09c7c524fe8a6df130483972766f843<br>**SHA-256 :** ddf43c46416e84f79cad1643a0b7a39c9aa4b50a<br>**SHA-512 :** 8d41def16f23e003b95c36ea8317c882918a8264<br>**Size :** 0.201 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F5F320A94D4D2B4465D8F17E2BB2D351_49C072E510849BAED98CE9762AC0F3EF** | **Type :** data<br>**MD5 :** d1879eed958e27f4d36503ff4511728d<br>**SHA-1 :** 56f13a332eae43e9faaf82f3a1992e7098a8c48b<br>**SHA-256 :** 081742bba12f0151e2ede08291662bd17f64d693<br>**SHA-512 :** d60614b391955379079774ca01136051913d714<br>**Size :** 0.463 Kilobytes. |
| **C:\Users\User\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012018072320180724\Index.Dat** | **Type :** Internet Explorer cache file version Ver 5.2<br>**MD5 :** 83cd904564774a3a2b22eb376f9c2853<br>**SHA-1 :** 90f22fcd66a310f374ebf20e721e60ca7a49bd3f<br>**SHA-256 :** d1378092e942ddab31c7ea4520de686dbb79101<br>**SHA-512 :** 4caae079c97b6b6585a45c43e156211b8310dcfc<br>**Size :** 32.768 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F5F320A94D4D2B4465D8F17E2BB2D351_D4C7B7247BFF9536583C1237360C2363** | **Type :** data<br>**MD5 :** 828b0fdb02c97c5c7946f360ca91a9eb<br>**SHA-1 :** 5d71e48fa2fc137b57f71dfb98f679879cc7cf3a<br>**SHA-256 :** 17d5ee30297841156a105ff76aed1151cd213c77<br>**SHA-512 :** d9ad3e67cd151ac2aa8fde82c18119b5dba63e49<br>**Size :** 0.463 Kilobytes. |
| **C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Index.Dat** | **Type :** Internet Explorer cache file version Ver 5.2<br>**MD5 :** 678c2256d3d54795ab7d108a0bd23abc<br>**SHA-1 :** 3b61366ba9cdad94eef7672dafd51f6b34d05d4c<br>**SHA-256 :** 9ba99139130395d95cc7395a3e7f58ebbba1a2ec<br>**SHA-512 :** 2c85e6fdd3a640b6d8e43d2660c4a90dfb8723ae<br>**Size :** 180.224 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EDC238BFF48A31D55A97E1E93892934B_C20E0DA2D0F89FE526E1490F4A2EE5AB** | **Type :** data<br>**MD5 :** cf17335341becbe3f008d936a191eb07<br>**SHA-1 :** 16bf2e1493966fae2df8f9f4d726272176c10037<br>**SHA-256 :** 4862f020eb2a85b2282d9eeb90f5ed3bf2c494c5<br>**SHA-512 :** 305b1dd8df4039d84fcd654ea49ab2691dd0e439<br>**Size :** 0.471 Kilobytes. |
| **C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\Authorization[1].Css** | **Type :** very short file (no magic)<br>**MD5 :** 68b329da9893e34099c7d8ad5cb9c940<br>**SHA-1 :** adc83b19e793491b1c6ea0fd8b46cd9f32e592fc<br>**SHA-256 :** 01ba4719c80b6fe911b091a7c05124b64eeece96<br>**SHA-512 :** be688838ca8686e5c90689bf2ab585cef1137c99<br>**Size :** 0.001 Kilobytes. |
| **C:\Users\User\AppData\Roaming\Microsoft\Windows\IETldCache\Index.Dat** | **Type :** Internet Explorer cache file version Ver 5.2<br>**MD5 :** 73f66dbeea4b5833334065f993ae561a<br>**SHA-1 :** 867f37a1dc85bafe6633165b3fab2f7965412afa<br>**SHA-256 :** baf57b866794ac49e94b046b783f96109b3f73cd<br>**SHA-512 :** c15aa8321e9f84672479c17b05a1f58222ee44a6<br>**Size :** 262.144 Kilobytes. |

| FILE PATH | TYPE AND HASHES |
|---|---|
| **C:\Users\User\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6FDD3035-8DC5-11E8-9C49-080027CB305F}.Dat** | **Type :** Composite Document File V2 Document, No summary info<br>**MD5 :** 79cd4dd4b4b407c06ac854986ddb18cd<br>**SHA-1 :** f11a966751ac2a0f5556d4106877eb34295ce69d<br>**SHA-256 :** 14429b11cab54814e4727ebf1256440475daf0c5<br>**SHA-512 :** 2fb1c8bc9d19eb7f59ae99e6a51199ce3922c6dc<br>**Size :** 4.608 Kilobytes. |
| **C:\Users\User\AppData\Local\Microsoft\Windows\History\History.IE5\Index.Dat** | **Type :** Internet Explorer cache file version Ver 5.2<br>**MD5 :** cdbfe85659a8fde87a94fc301bca4da8<br>**SHA-1 :** aee9d5ec71e5d10890cd9075ede593e9a13eef9c<br>**SHA-256 :** c851ebc1caca8d62ea718acbbc00853835dfd68b<br>**SHA-512 :** 11cb235d4406fb7976b9bbe1cf97f6c4bd39dbf7<br>**Size :** 49.152 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EDC238BFF48A31D55A97E1E93892934B_C20E0DA2D0F89FE526E1490F4A2EE5AB** | **Type :** data<br>**MD5 :** 638a75506254c509f9bf046078c5ed81<br>**SHA-1 :** 126e773c10091db56d7dd69d01f457a94b81f11c<br>**SHA-256 :** c1c3486a1d109cfa025dc1e7e036a2e215c8f444<br>**SHA-512 :** 0ed9d332659627dea557ccd8af3b60710d0a0b7(<br>**Size :** 0.426 Kilobytes. |
| **C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\3658603751-Ieretrofit[1].Js** | **Type :** ASCII text, with very long lines<br>**MD5 :** 5cbe54ee3aba54b2d177109f29e0aa02<br>**SHA-1 :** 69dce205aad700d209ccca065e77b2f3d68fb67a<br>**SHA-256 :** caa036d65ab908f96df47f5bbe22fae1504b5b73<br>**SHA-512 :** 96a459395d2f2321b88571546e7838ba76abba3<br>**Size :** 36.717 Kilobytes. |
| **C:\Users\User\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{6FDD3034-8DC5-11E8-9C49-080027CB305F}.Dat** | **Type :** Composite Document File V2 Document, No summary info<br>**MD5 :** 0c821ffa1753747078ef4b076fd015af<br>**SHA-1 :** 3c48613ac6a69ccbf8d490316f4835eaa059312e<br>**SHA-256 :** d5b6d893fc89374d85fd4cb420f5a9d914c74695<br>**SHA-512 :** e042d6f242881cc273600a13055c755099910950<br>**Size :** 3.584 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\BEC6224B02D155A396218A2504F3EE0B** | **Type :** data<br>**MD5 :** d4db052864361f5c197982ad25c98b4c<br>**SHA-1 :** aadd099acc1bab124a4cc52cb1914bd493b22b7c<br>**SHA-256 :** 61251848e0e8fbed2e7b4c3ee7e7b21b4d2c235<br>**SHA-512 :** 013322e52d8a6bd224ea90f9ea7ab6c60d82bc47<br>**Size :** 0.236 Kilobytes. |
| **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CFE86DBBE02D859DC92F1E17E0574EE8_FDB452422670E72EDD3FB3D65568F821** | **Type :** data<br>**MD5 :** d9d754520ae3340aa37cca6115eee05b<br>**SHA-1 :** a0320372760d99c762cb2eb4b37f776625ef1b33<br>**SHA-256 :** 7dc8284c51c9a38dc1bf03bd28857ea5336e8f5c<br>**SHA-512 :** 440f6a9ea2ce5ecd1fd7cb3d122a6f5f108550d71<br>**Size :** 0.468 Kilobytes. |

## MATCH YARA RULES

| MATCH RULES |
|---|

## STATIC FILE INFO

| | |
|---|---|
| **File Name:** | None |
| **File Type:** | HTML document, ASCII text, with very long lines |
| **SHA1:** | 849a058cf92f0ae31320d42f3cb06b1585a26386 |
| **MD5:** | 122c913d14c61dea54182320cf6ae3a4 |
| **First Seen Date:** | 2018-07-22 06:14:25.627324 ( 10 months ago ) |
| **Number Of Clients Seen:** | 1 |
| **Last Analysis Date:** | 2018-07-22 06:14:25.627324 ( 10 months ago ) |
| **Human Expert Analysis Date:** | 2019-03-01 12:54:28.975464 ( 3 months ago ) |
| **Human Expert Analysis Result:** | Malware |

## DETAILED FILE INFO

### ADDITIONAL FILE INFORMATION

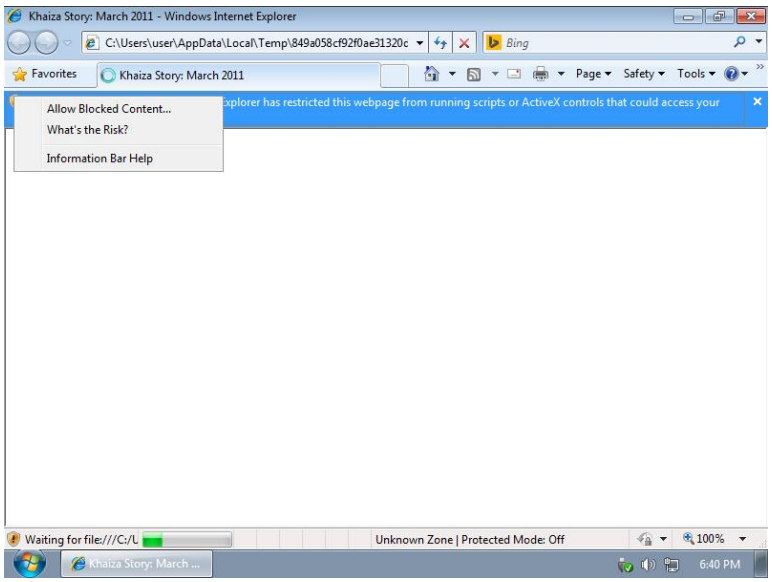
#### PE Headers

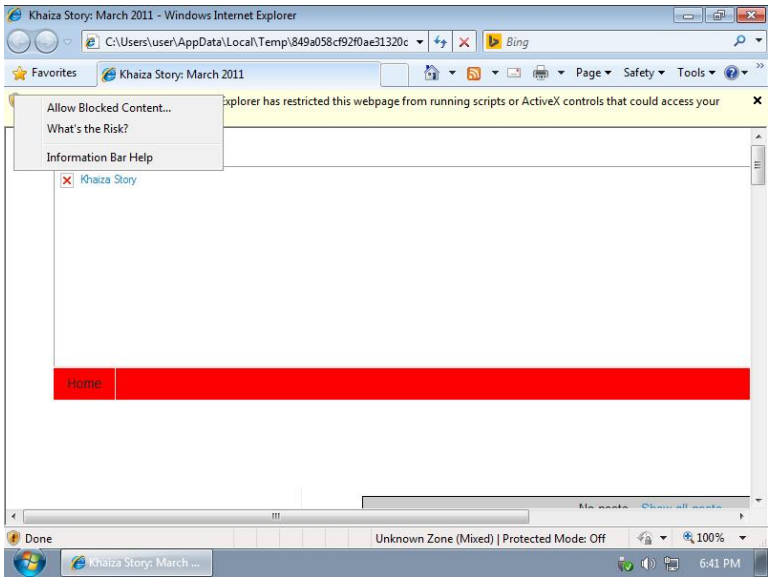
| PROPERTY | VALUE |
|---|---|
| Magic Literal Enum | 14 |
| File Type Enum | 1 |
| File Size | 71999 |
| Sha256 | 2b8ed16ef35af5bfa10175ace70a9ffcf28d74fd5cfbd65a2718a66aa78888c9 |
| Mime Type | text/html |

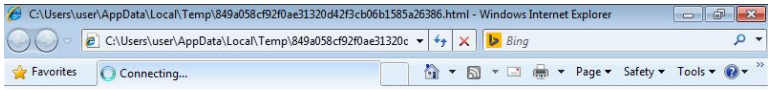
### CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

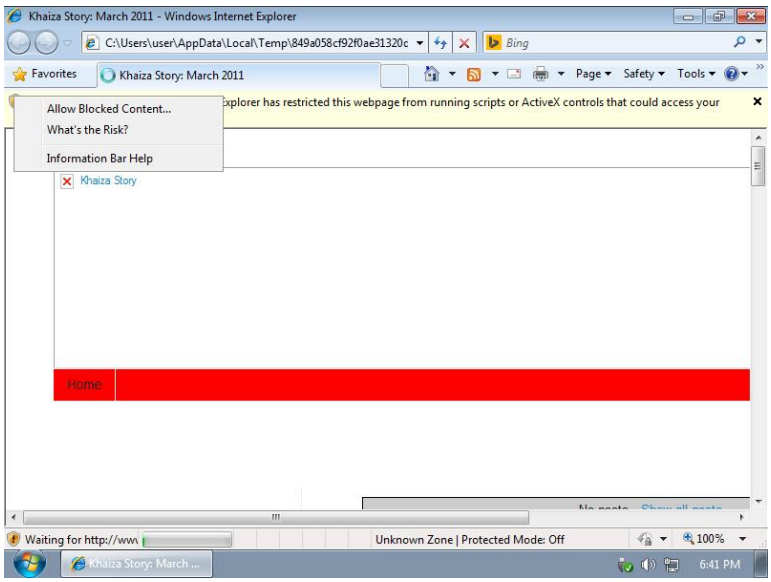
## SCREENSHOTS

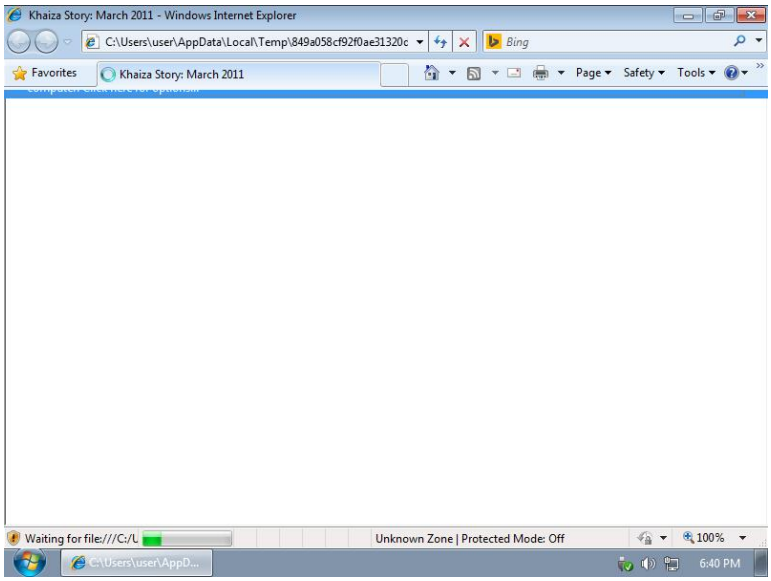


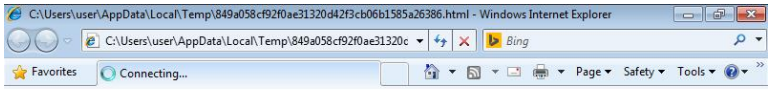

Khaiza Story: March 2011 - Windows Internet Explorer
C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320c
Bing
Favorites
Khaiza Story: March 2011
Page
Safety
Tools
Allow Blocked Content...
What's the Risk?
Information Bar Help
Khaiza Story
Home
Done
Unknown Zone (Mixed) | Protected Mode: Off
100%
6:41 PM


C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320d42f3cb06b1585a26386.html - Windows Internet Explorer
C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320c
Bing
Favorites
Connecting...
Page
Safety
Tools

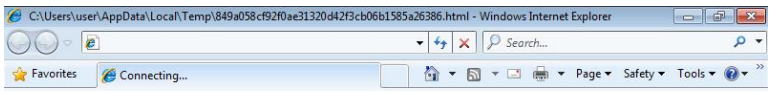

100%
6:39 PM


Khaiza Story: March 2011 - Windows Internet Explorer
C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320c
Bing
Favorites
Khaiza Story: March 2011
Page
Safety
Tools
Allow Blocked Content...
What's the Risk?
Information Bar Help
Khaiza Story
Home
Waiting for http://ww
Unknown Zone | Protected Mode: Off
100%
6:41 PM

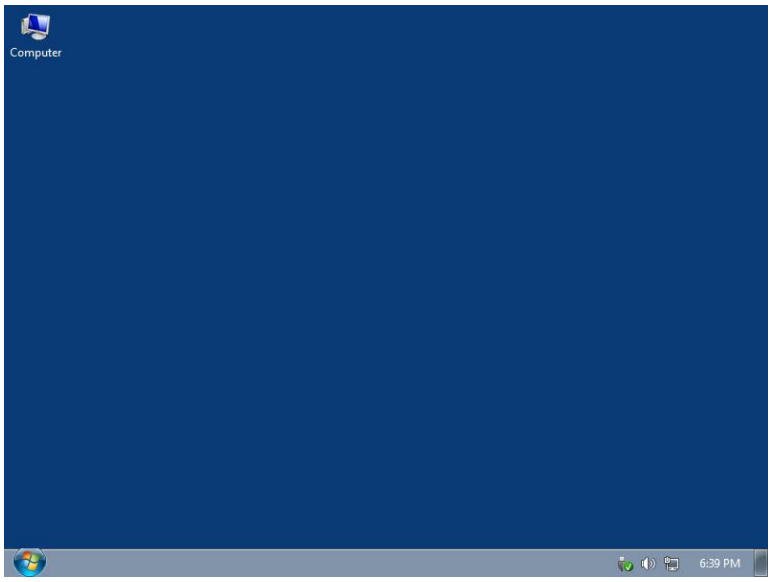

Khaiza Story: March 2011 - Windows Internet Explorer
C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320c
Bing
Favorites
Khaiza Story: March 2011
Page
Safety
Tools
Waiting for file:///C:/L
Unknown Zone | Protected Mode: Off
100%
6:40 PM

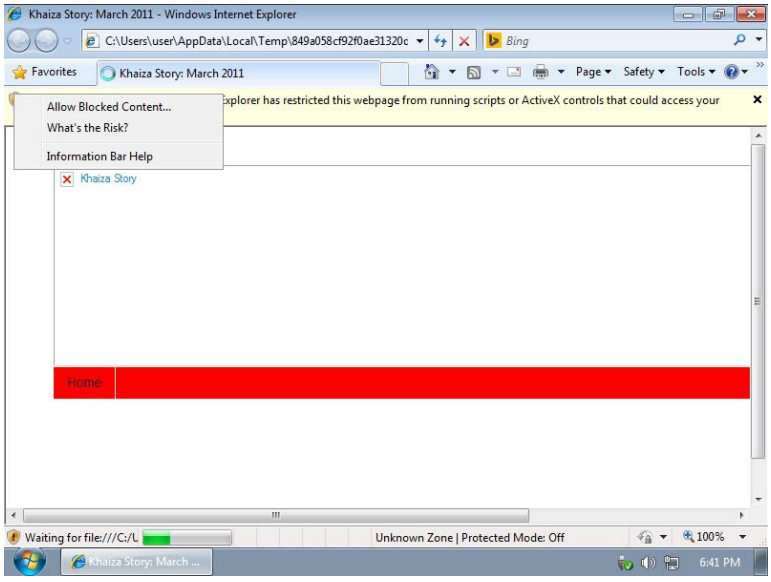

C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320d42f3cb06b1585a26386.html - Windows Internet Explorer
C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320c
Bing
Favorites
Connecting...
Page
Safety
Tools

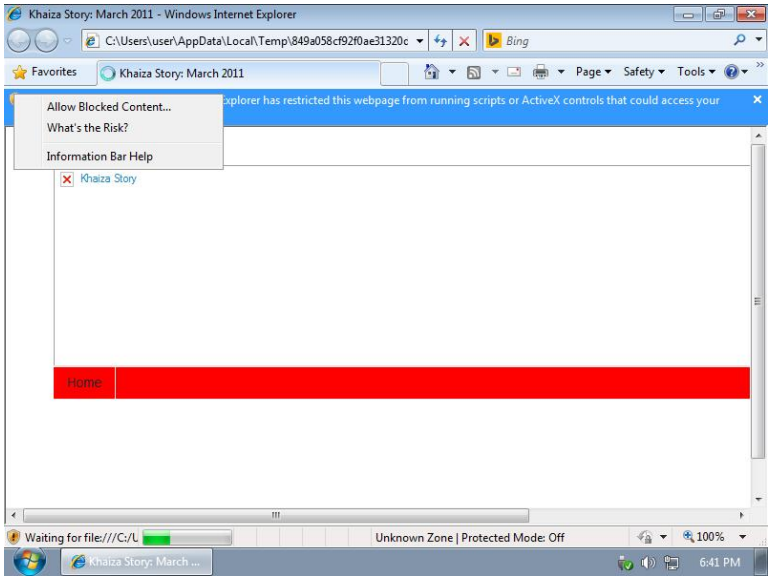

100%
6:39 PM

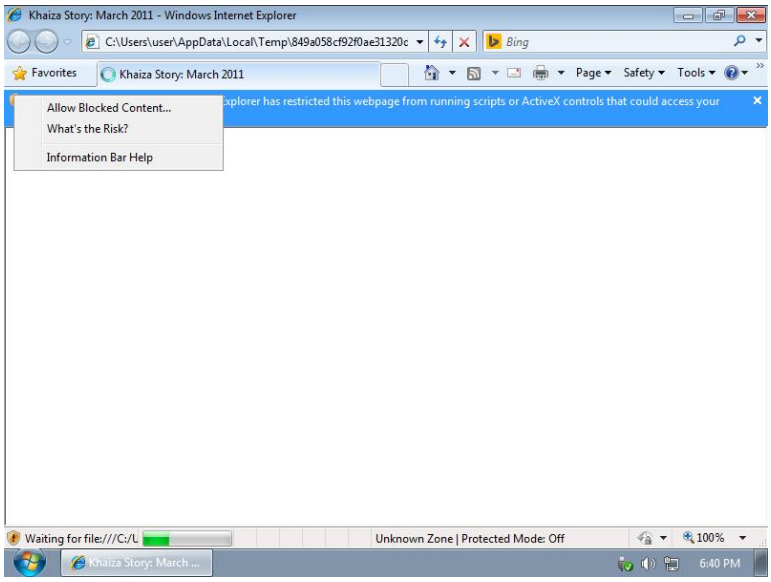

C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320d42f3cb06b1585a26386.html - Windows Internet Explorer
Search...
Favorites
Connecting...
Page
Safety
Tools

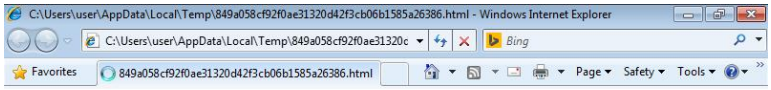

Windows Internet Ex...
6:39 PM


Computer
6:39 PM

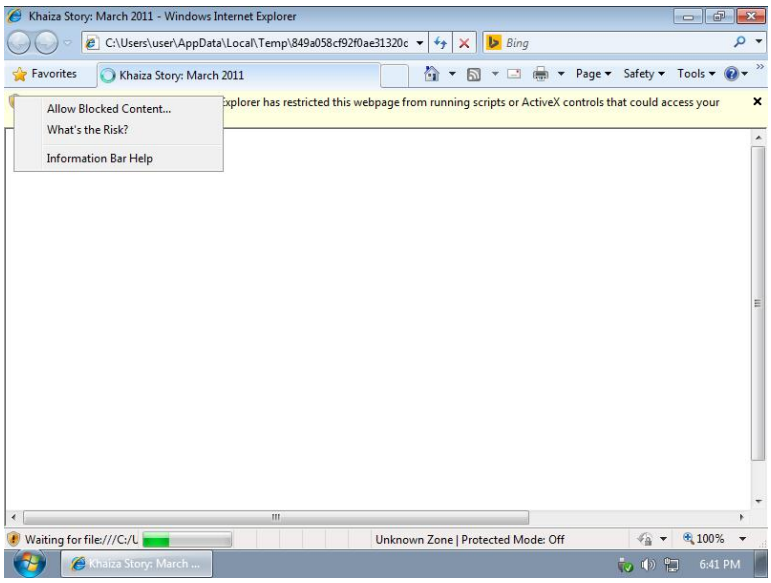

Khaiza Story: March 2011 - Windows Internet Explorer
C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320c
Bing
Favorites
Khaiza Story: March 2011
Page
Safety
Tools
Allow Blocked Content...
What's the Risk?
Information Bar Help
Khaiza Story
Home
Waiting for file:///C:/L
Unknown Zone | Protected Mode: Off
100%
Khaiza Story: March ...
6:41 PM

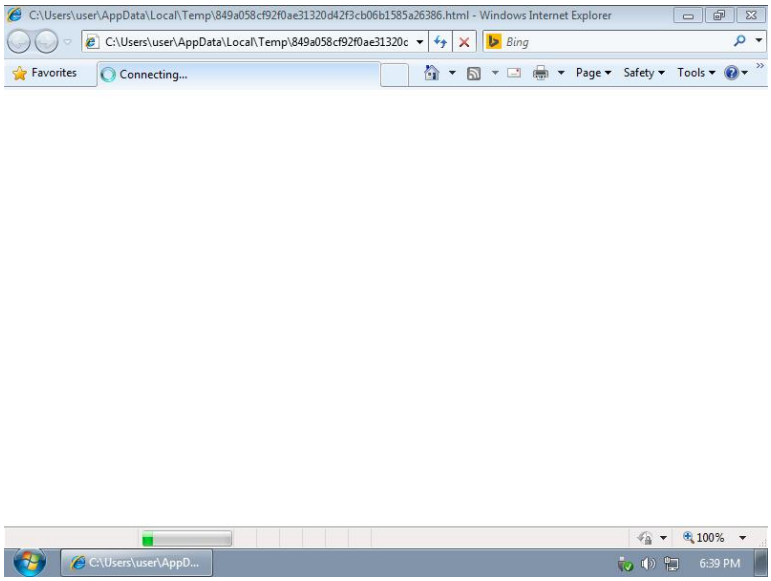

Khaiza Story: March 2011 - Windows Internet Explorer
C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320c
Bing
Favorites
Khaiza Story: March 2011
Page
Safety
Tools
Allow Blocked Content...
What's the Risk?
Information Bar Help
Khaiza Story
Home
Waiting for file:///C:/L
Unknown Zone | Protected Mode: Off
100%
Khaiza Story: March ...
6:41 PM


Khaiza Story: March 2011 - Windows Internet Explorer
C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320c
Bing
Favorites
Khaiza Story: March 2011
Page
Safety
Tools
Allow Blocked Content...
What's the Risk?
Information Bar Help
Waiting for file:///C:/L
Unknown Zone | Protected Mode: Off
100%
6:40 PM


C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320d42f3cb06b1585a26386.html - Windows Internet Explorer
C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320c
Bing
Favorites
849a058cf92f0ae31320d42f3cb06b1585a26386.html
Page
Safety
Tools


Waiting for file:///C:/Users
Unknown Zone | Protected Mode: Off
100%
6:40 PM


Khaiza Story: March 2011 - Windows Internet Explorer
C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320c
Bing
Favorites
Khaiza Story: March 2011
Page
Safety
Tools
Allow Blocked Content...
What's the Risk?
Information Bar Help
Waiting for file:///C:/L
Unknown Zone | Protected Mode: Off
100%
6:41 PM


C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320d42f3cb06b1585a26386.html - Windows Internet Explorer
C:\Users\user\AppData\Local\Temp\849a058cf92f0ae31320c
Bing
Favorites
Connecting...
Page
Safety
Tools
100%
C:\Users\user\AppD...
6:39 PM