Brighton-Colorado-Blacklisted-Cyber-Attacker-against-Stew-Webb-September-23-2020

Brighton, Colorado, United States was blocked by real-time IP blacklist at http:// stewwebb.com/ wp-login.php

9/23/2020 10:25:55 PM (10 hours 43 mins ago)

IP: 173.8.240.211 Hostname: 173-8-240-211-Colorado.hfc.comcastbusiness.net

Human/Bot: Bot

Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101 Firefox/62.0

Type: Blocked

Brighton, Colorado, United States was blocked by real-time IP blacklist at http:// stewwebb.com/ wp-login.php

9/23/2020 10:25:54 PM (10 hours 43 mins ago)

IP: 173.8.240.211 Hostname: 173-8-240-211-Colorado.hfc.comcastbusiness.net

Human/Bot: Bot

Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101 Firefox/62.0

Colorado

China Tencents

Cyber Attacker

United States visited http://www.stewwebb.com/

9/24/2020 7:35:14 AM (57 minutes ago)

IP: 45.42.85.138 Hostname: 45.42.85.138

Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36

NetRange: 45.42.80.0 - 45.42.95.255

[4096 addresses in this network]

CIDR: 45.42.80.0/20 (45.42.80.0 - 45.42.95.255)

[4096 addresses in this network]

NetName: XT-01

NetHandle: NET-45-42-80-0-1

Parent: NET45 (NET-45-0-0-0-0)

NetType: Direct Allocation

OriginAS: AS21684

Organization: XIATIAN.LLC (XIATI)

RegDate: 2015-03-09

Updated: 2015-03-09

Ref: https://rdap.arin.net/registry/ip/45.42.80.0

OrgName: XIATIAN.LLC

OrgId: XIATI

Address: 2208 W.2ND Street

City: Florence

StateProv: CO

PostalCode: 81226

Country: US

RegDate: 2015-01-20

Updated: 2017-01-28

Ref: https://rdap.arin.net/registry/entity/XIATI

OrgTechHandle: ZHENG40-ARIN

OrgTechName: Zhen, Guo

OrgTechPhone: +1-812-333-1324

OrgTechEmail: tech@rhuq.com

OrgTechRef: https://rdap.arin.net/registry/entity/ZHENG40-ARIN

OrgAbuseHandle: ZHENG37-ARIN

OrgAbuseName: Zhen, Guo

OrgAbusePhone: +1-812-333-1324

OrgAbuseEmail: idc-client@outlook.com

OrgAbuseRef: https://rdap.arin.net/registry/entity/ZHENG37-ARIN

OrgNOCHandle: ZHENG39-ARIN

OrgNOCName: Zhen, Guo

OrgNOCPhone: +1-812-333-1324

OrgNOCEmail: noc@rhuq.com

OrgNOCRef: https://rdap.arin.net/registry/entity/ZHENG39-ARIN

rhuq.com

rhuq.com

Domain rhuq.com is not listed in the top million list of Alexa. It is not listed in the DMOZ directory. This domain is hosted by Cloudflare, Inc. (AS13335). The first DNS server is nash.ns.cloudflare.com. The current IPv4 address is 104.27.182.47. The mail server with the highest priority is mxbiz1.qq.com.

A / AAAA Record	Provider	ASN
104.27.182.47 (US us flag)		
Cloudflare, Inc. (US us flag)	AS13335	
104.27.183.47 (US us flag)		
Cloudflare, Inc. (US us flag)	AS13335	
172.67.214.3 (US us flag)		
Cloudflare, Inc. (US us flag)	AS13335	
2606:4700:3035::681b:b72f (US us flag)		
Cloudflare, Inc. (US us flag)	AS13335	
2606:4700:3035::ac43:d603 (US us flag)		
Cloudflare, Inc. (US us flag)	AS13335	
2606:4700:3037::681b:b62f (US us flag)		
Cloudflare, Inc. (US us flag)	AS13335	

NS Record	IP Address	Provider	ASN
nash.ns.cloudflare.com			
	108.162.193.209 (US us flag)	Cloudflare, Inc. (US us flag)	AS13335
	172.64.33.209 (US us flag)	Cloudflare, Inc. (US us flag)	AS13335
	173.245.59.209 (US us flag)	Cloudflare, Inc. (US us flag)	AS13335
	2606:4700:58::adf5:3bd1 (US us flag)	Cloudflare, Inc. (US us flag)	AS13335
	2803:f800:50::6ca2:c1d1 (CR cr flag)	Cloudflare, Inc. (US us flag)	AS13335
	2a06:98c1:50::ac40:21d1 (GB gb flag)	Cloudflare, Inc. (US us flag)	AS13335
ullis.ns.cloudflare.com			

108.162.194.127 (US us flag) Cloudflare, Inc. (US us flag) AS13335

162.159.38.127 Cloudflare, Inc. (US us flag) AS13335

172.64.34.127 (US us flag) Cloudflare, Inc. (US us flag) AS13335

2606:4700:50::a29f:267f (US us flag) Cloudflare, Inc. (US us flag) AS13335

2803:f800:50::6ca2:c27f (CR cr flag) Cloudflare, Inc. (US us flag) AS13335

2a06:98c1:50::ac40:227f (GB gb flag) Cloudflare, Inc. (US us flag) AS13335

MX Record IP Address Provider ASN

mxbiz1.qq.com (pref: 5)

203.205.232.191 (CN cn flag) Shenzhen Tencent Computer Systems Company Limited (CN cn flag) AS132203

mxbiz2.qq.com (pref: 10)

61.241.49.98 (CN cn flag) China Unicom Shenzen network (CN cn flag) AS17623

163.177.89.176 (CN cn flag) China Unicom Shenzen network (CN cn flag) AS17623

No SPF record found for this domain.

Domain Name: RHUQ.COM

Registry Domain ID: 1829742825_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.ename.com

Registrar URL: http://www.ename.net

Updated Date: 2020-07-30T07:59:38Z

Creation Date: 2013-10-03T10:00:04Z

Registry Expiry Date: 2021-10-03T10:00:04Z

Registrar: eName Technology Co., Ltd.

Registrar IANA ID: 1331

Registrar Abuse Contact Email: removed email address

Registrar Abuse Contact Phone: 86.4000044400

Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Name Server: NASH.NS.CLOUDFLARE.COM

Name Server: ULLIS.NS.CLOUDFLARE.COM

DNSSEC: unsigned

name.com