

Forum:[Hack Forums](#)

Thread: [Possible Botnet connection](#)

well then - October 14, 2014, 6:18 pm

Apparently my other thread was deleted.

Getting this on my p2p blocker.

Does that mean I am connected to a botnet? If so, what are the steps to removing it?

koolfrank - October 14, 2014, 6:36 pm

your program blocked the "botnet on smart broadband"..doesn't mean your connected to a botnet... you'll see that alot if your torrenting..

Aura - October 14, 2014, 6:43 pm

(Oct 14, 2014 06:36 PM)koolfrank Wrote: [\[CITE\]](#) your program blocked the "botnet on smart broadband"..doesn't mean your connected to a botnet... you'll see that alot if your torrenting.. This. We had a thread with that kind of issue a few months ago. I can't remember what it was exactly too but it wasn't a botnet.

Code #

ARIN WHOIS data and services are subject to the Terms of Use

available at: https://www.arin.net/whois_tou.html

#

If you see inaccuracies in the results, please report at

<http://www.arin.net/public/whoisinaccuracy/index.xhtml>

#

#

The following results may also be obtained via:

<http://whois.arin.net/rest/nets;q=85.143.114.220?showDetails=true&showARIN=false&ext=netref2>

#

NetRange: 85.0.0.0 - 85.255.255.255

CIDR: 85.0.0.0/8

OriginAS:

NetName: 85-RIPE

NetHandle: NET-85-0-0-0-1

Parent:

NetType: Allocated to RIPE NCC

Comment: These addresses have been further assigned to users in

Comment: the RIPE NCC region. Contact information can be found in

Comment: the RIPE database at <http://www.ripe.net/whois>

RegDate: 2004-04-01

Updated: 2009-05-18

Ref: <http://whois.arin.net/rest/net/NET-85-0-0-0-1>

OrgName: RIPE Network Coordination Centre

OrgId: RIPE

Address: P.O. Box 10096
City: Amsterdam
StateProv:
PostalCode: 1001EB
Country: NL
RegDate:
Updated: 2013-07-29
Ref: <http://whois.arin.net/rest/org/RIPE>

ReferralServer: whois://whois.ripe.net:43

OrgTechHandle: RNO29-ARIN
OrgTechName: RIPE NCC Operations
OrgTechPhone: +31 20 535 4444
OrgTechEmail: hostmaster@ripe.net
OrgTechRef: <http://whois.arin.net/rest/poc/RNO29-ARIN>

OrgAbuseHandle: ABUSE3850-ARIN
OrgAbuseName: Abuse Contact
OrgAbusePhone: +31205354444
OrgAbuseEmail: abuse@ripe.net
OrgAbuseRef: <http://whois.arin.net/rest/poc/ABUSE3850-ARIN>

ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/whois_tou.html

If you see inaccuracies in the results, please report at
<http://www.arin.net/public/whoisinaccuracy/index.xhtml>
#

Deferred to specific whois server: whois.ripe.net...

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See <http://www.ripe.net/db/support/db-terms-conditions.pdf>

% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.

% Information related to '85.143.112.0 - 85.143.115.0'

% Abuse contact for '85.143.112.0 - 85.143.115.0' is 'abuse@runnet.ru'

inetnum: 85.143.112.0 - 85.143.115.0
netname: MEPHI
descr: National Research Nuclear University 'MEPhI'
descr: 31 Kashirskoe shosse
descr: 115409 Moscow
country: RU
admin-c: RV13-RIPE

tech-c: PM15940-RIPE
status: ASSIGNED PA
mnt-by: RUNNET-MNT
source: RIPE # Filtered

person: Petr Makarov
address: National research nuclear university 'MEPhI'
address: 31 Kashirskoe shosse
address: 115409 Moscow
address: Russia
phone: +7 (495) 7885699
nic-hdl: PM15940-RIPE
mnt-by: RUNNET-MNT
source: RIPE # Filtered

person: Raisa Y Voronina
address: National research nuclear university 'MEPhI'
address: 31 Kashirskoe shosse
address: 115409 Moscow
address: Russia
phone: +7 495 3239493
nic-hdl: RV13-RIPE
mnt-by: RADIO-MSU-MNT
source: RIPE # Filtered

% Information related to '85.142.0.0/15AS3267'

route: 85.142.0.0/15
descr: RUNNet
descr: Russian Federal University Network
origin: AS3267
mnt-by: RUNNET-MNT
mnt-routes: RUNNET-MNT
mnt-routes: AS3343-MNT { 85.142.20.0/24 }
mnt-routes: TULSU-ISP-MNT { 85.142.128.0/20 }
mnt-routes: MISIS-MNT { 85.143.100.0/24 }
mnt-routes: MISIS-MNT { 85.143.104.0/22 }
source: RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.75 (DB-4)

-Hyperion - October 14, 2014, 7:00 pm

Your torrent client is just connecting to a peer who is in a botnet is all.

-sent from my iPhone