

Forum:[Hack Forums](#)

Thread: [RATs: How to cloudflare your RATs DNS ? Will this work](#)

cashf - December 24, 2016, 6:12 pm

Hey guys...

I am wondering: Is this possible ??

Point is: You can hide your websites IP so that noone finds your IP. Just setup a proper Cloudflare or Incapsula setup and there you go.

My idea is: Why don't we do this for a RATs DNS, too. Say for example:

- 1) I register 2 cheap domains and point them to my VPSs IP, there my RAT has his C&C.
- 2) Now I put both domains to Cloudflare/Incapsula. Now my 2 domains DNS point to a cloudflare/incapsula IP. Now all my slaves can only see the cloudflare/incapsula IP, but not the real C&C IP. Therefore my C&C IP is much more protected and they cannot find the hosting of my C&C.
- 3) Now only Cloudflare/Incapsula know my real VPS IP (my RATs C&C). So they forward all the traffic between my slaves and my C&C.

It would look like that:

Slaves <-> Cloudflare/Incapsula <-> my C&C

Question: WOULD THIS WORK ? Did anyone try such a setup before?

Or will Cloudflare/Incapsula block the necessary ports and limit the traffic forwarding to some port80 shit ??

Thanks a lot for your ideas and discussion..

cashf ?

Have a great Christmas guys ?

Lucrid - December 24, 2016, 6:15 pm

I highly doubt this would work, cloud flare is just for web services if I'm not mistaken.

SIM-2053312 - December 24, 2016, 6:17 pm

I don't think this would work but if they did , your cloud flare would probably be banned since a lot of reports would be to that ip

Ainaj - December 24, 2016, 6:25 pm

CF just proxies HTTP content.

Maxie - December 24, 2016, 6:28 pm

I think it would be possible if you did this:

HTTP server that commands the bots (by sending simple commands in HTTP headers/echos it on the page)

hosted on cloudflare
create a rat that can read commands from a server and execute them
link to cloudflare

But if you don't have any coding experience, I guess this suddenly turns pretty impossible.

Edit: You could also make a program that runs on your VPS that reads from the server -> executes the command on the rat.

But it would still require some programming and eventual injection into the rat client.

cashf - December 24, 2016, 6:33 pm

Yeah.... thanks guys... I also found this info

support.cloudflare.com/hc/en-us/articles/200169156-Which-ports-will-CloudFlare-work-with-

Looks that the ports that Cloudflare forwards are pretty limited :(

Nickname. - December 26, 2016, 2:44 pm

(Dec 24, 2016 07:25 PM)CesarVB Wrote: [\[CITE\]](#) CF just proxies HTTP content.
Wrong!

QU?CKSILVER - December 26, 2016, 3:03 pm

This will not work, as bots will still have a direct connection to you. IP address will still be revealed.

#Skyline - December 26, 2016, 3:11 pm

(Dec 26, 2016 04:03 PM)QU?CKSILVER Wrote: [\[CITE\]](#) This will not work, as bots will still have a direct connection to you. IP address will still be revealed.

It will work.

The TCP connection will point to cloudflare DNS, whilst routing all traffic to the original host.

QU?CKSILVER - December 26, 2016, 3:22 pm

(Dec 26, 2016 04:11 PM)#Skyline? Wrote: [\[CITE\]](#) It will work.

The TCP connection will point to cloudflare DNS, whilst routing all traffic to the original host.

Cloudflare needs to act as a TCP proxy in order for this to happen, not just a connection forwarder, which I really doubt they do.

cashf - December 26, 2016, 8:21 pm

Well, quite a discussion here. I would say 80% that it will not work, but I never tried. Anyone wants to test it out?

Ainaj - December 26, 2016, 8:34 pm

(Dec 26, 2016 09:21 PM)cashf Wrote: [\[CITE\]](#) Well, quite a discussion here. I would say 80% that it will not work, but I never tried. Anyone wants to test it out?

It just wont work, cloudflare proxies HTTP data. The dns resolves to one of their IPs, and depending on the HOST header provided it'll go to the origin web server.

This wont work for a rat since it they use raw tcp/udp packets, not http packets (which contain a HOST header).

But sure, lets test it.

104.27.176.251 is not my IP address, it's one of cloudflares proxy servers. Now since it's not a valid

HTTP request, cloudflare ignores it, so no connection is made.

However, if I run a webserver on the same port it works since your browser sends the HOST header (your dns/domain in this instance) and cloudflare knows what to do with it.

If you want this to work you will have to use a rat that is designed around the HTTP protocol, it is completely possible, but completely stupid.

KN. Strike - December 26, 2016, 8:43 pm

(Dec 24, 2016 07:25 PM)CesarVB Wrote: [\[CITE\]](#) CF just proxies HTTP content. You can put crypted contents into HTTP content, which will make it go through CF without CF being able to see what the content uncrypted.

You can put any protocol(or substitute) into a HTTP, just need to know how to do it. Need a program on your server to interpret it too

Ainaj - December 26, 2016, 8:49 pm

(Dec 26, 2016 09:43 PM)KN. Strike Wrote: [\[CITE\]](#) You can put crypted contents into HTTP content, which will make it go through CF without CF being able to see what the content uncrypted.

You can put any protocol(or substitute) into a HTTP, just need to know how to do it. Need a program on your server to interpret it too

Pretty sure I covered that in my post, just add the HEAD header (which would mean make your packets valid HTTP packets).

(Dec 26, 2016 09:46 PM)Yani Wrote: [\[CITE\]](#) Please enlighten us.

As far as I know even websockets don't work with cloudflare.
Even webrequests use sockets, it'll work with enough know-how.

KN. Strike - December 26, 2016, 8:52 pm

(Dec 26, 2016 09:46 PM)Yani Wrote: [\[CITE\]](#) Please enlighten us.

As far as I know even websockets don't work with cloudflare.

I think you don't see what I mean. The R.A.T. get all information about a slave, he puts them into a http file and send it to the master. The master then send all informations he has to send through HTTP too to the R.A.T. program. Just need both program to know how to interpret the informations they get through the HTTP files.

You don't send commands directly to the slave, you send informations to the R.A.T. that then will take actions.

In theory that's possible, I've talked about it with my teacher in programmation. I started IT school 2 weeks ago and had a similar question ^^

- All informations sent must be crypted before being put in the HTTP file, so Cloudflare will not in the future be able to decrypt it.

#Skyline - December 26, 2016, 8:53 pm

(Dec 26, 2016 09:43 PM)KN. Strike Wrote: [\[CITE\]](#) You can put crypted contents into HTTP content, which will make it go through CF without CF being able to see what the content uncrypted.

You can put any protocol(or substitute) into a HTTP, just need to know how to do it. Need a program on your server to interpret it too

That's the only way I was capable of doing it.

? [\$(1000)\$] ? - December 26, 2016, 8:56 pm

Just use a dns... a free one...

KN. Strike - December 26, 2016, 8:58 pm

(Dec 26, 2016 09:56 PM)? [\$(1000)\$] ? Wrote: [\[CITE\]](#) Just use a dns... a free one...

When you check Wireshark. If you see packets going to Cloudflare you won't suspect it. A free dns is easily spotted.

? [\$(1000)\$] ? - December 26, 2016, 9:02 pm

Ahhhhh got ya now

Wow is it possible seems very smart

cashf - December 27, 2016, 7:17 pm

Thanks guys for the info. I think... well the idea is pretty nice. Just think about hiding the RATs traffic within cloudflare traffic. Noone would out of the box see that this is RAT traffic. Just well... needs some coding I think.... any RAT developer who wants to implement this ? Somehow the idea wouldn't be bad:

1) cloudflare traffic would be very unsuspicious

2) IP of your c&c would be protected behind cloudflare. WOW.... this is something !!

Have a great day guys...