

Forum:[Hack Forums](#)

Thread: [RATs: DNS stole all my slaves by pointing DNS to some other IP... WTF ??](#)

cashf - December 24, 2016, 6:00 pm

Hey Guys,

I saw something REALLY interstesting:

1) I started with Ratting a few days before. Got a nice spreading method which got me round about 100 slaves every 24 hours. This went on for 2 days.

2) On day 2 some Security Researcher, not a famous one, but some guy posted a warning online about my spreading method and that people should not download my RAT's server. He also uploaded my server to virustotal and published a couple of comments on virustotal about my spreading method.

3) Now some REALLY strange thing happened: Thing is... I put 2 free DNS (dynu.com) into my RAT. Today I woke up and saw that all my slaves had been gone. My first assumption was, that the DNS got deleted. But surprisingly this was NOT the case. Both DNS still pointed to my VPS and it all looked pretty fine.

Now I started to research and found this:

The DNS (dynu.com) had pointed my DNS to some OTHER IP (!!!). IP belongs to "Frontier Communications Corporation California Santa Monica". This lasted for 2-3 hours yesterday and then they reverted the DNS BACK TO MY original VPS IP !!!

My thought is now: WHAT THE FUCK IS THIS ??? Someone seems to PLAY WITH ME... ?

As far as my understanding goes... What could have happened is...

- 1) DNS pointed my RATs DNS to some other IP.
- 2) SOMEHOW they must have updated my slaves or did some other shit.

BECAUSE: Slaves do not connect any more. Slave count went from 200 to ZERO ??

I am not angry about it, and I was expecting something like that. But I was expecting that they would just DELETE my DNS, but here, they seem to play some dirty game with me.

ANYONE EXPERIENCED SOMETHING LIKE THAT ??

Have a great Christmas guys...

cashf ??

DTK-C - December 24, 2016, 6:57 pm

(Dec 24, 2016 07:00 PM)cashf Wrote: [\[CITE\]](#) Hey Guys,

I saw something REALLY interstesting:

1) I started with Ratting a few days before. Got a nice spreading method which got me round about 100 slaves every 24 hours. This went on for 2 days.

2) On day 2 some Security Researcher, not a famous one, but some guy posted a warning online about my spreading method and that people should not download my RAT's server. He also uploaded my server to virustotal and published a couple of comments on virustotal about my spreading method.

3) Now some REALLY strange thing happened: Thing is... I put 2 free DNS (dynu.com) into my RAT. Today I woke up and saw that all my slaves had been gone. My first assumption was, that the DNS got deleted. But surprisingly this was NOT the case. Both DNS still pointed to my VPS and it all looked pretty fine.

Now I started to research and found this:

The DNS (dynu.com) had pointed my DNS to some OTHER IP (!!!). IP belongs to "Frontier Communications Corporation California Santa Monica". This lasted for 2-3 hours yesterday and then they reverted the DNS BACK TO MY original VPS IP !!!

My thought is now: WHAT THE FUCK IS THIS ??? Someone seems to PLAY WITH ME... ?

As far as my understanding goes... What could have happened is...

- 1) DNS pointed my RATs DNS to some other IP.
- 2) SOMEHOW they must have updated my slaves or did some other shit.

BECAUSE: Slaves do not connect any more. Slave count went from 200 to ZERO ??

I am not angry about it, and I was expecting something like that. But I was expecting that they would just DELETE my DNS, but here, they seem to play some dirty game with me.

ANYONE EXPERIENCED SOMETHING LIKE THAT ??

Have a great Christmas guys...

cashf ??have fun behind bars lmao

Regulus - December 24, 2016, 6:59 pm

Doesn't sounds good at all.

Be careful when it comes to ratting.

Not sure why this happened but I'd keep a low profile.

Electrons - December 24, 2016, 7:01 pm

Doesn't look good mate. Relocate or fry your station.

Mitlar - December 24, 2016, 7:44 pm

As the user mentioned above I would keep low and destroy any suspicious shit on your computer. Encrypt your hard drives.

PixelatedBacon - December 24, 2016, 7:54 pm

ur so donezo m9. Destroy ur hardware or overclock ur own PC :)

NyQuil - December 24, 2016, 7:57 pm

doubt they stole your bots as when you build a rats file it is unique when it comes to the matter of a program using the data being sent back as well as the delimiter and password. even if they changed the IP to theres its not likely their using the same rat and password you are to connect to the hardcoded file on the clients computer.

Sheeple - December 24, 2016, 8:03 pm

(Dec 24, 2016 08:44 PM)L????? Wrote: [\[CITE\]](#) As the user mentioned above I would keep low and destroy any suspicious shit on your computer. Encrypt your hard drives.

Encrypting your hard drives would be the worst, and most pointless, thing to do.

Rhez - December 24, 2016, 8:29 pm

I think it's not possible to transfer the client to another because of the encrypted packets. ? Maybe you just lost the slave because of the changing IP.

JoshuTee - December 25, 2016, 12:35 am

They're probably going to try to steal your clients to uninstall your server

Purple Kief - December 25, 2016, 2:15 pm

"Frontier Communications Corporation California Santa Monica".

Research the shit out of that. If it's legit I'd prepare your buttohole.

eightz - December 25, 2016, 2:22 pm

(Dec 25, 2016 03:15 PM)Purple Kief Wrote: [\[CITE\]](#) "Frontier Communications Corporation California Santa Monica".

Research the shit out of that. If it's legit I'd prepare your buttohole.

It's a telecommunications company. Provides internet, home phone, etc

https://en.m.wikipedia.org/wiki/Frontier_Communications

Purple Kief - December 25, 2016, 2:33 pm

(Dec 25, 2016 03:22 PM)eightz Wrote: [\[CITE\]](#) It's a telecommunications company. Provides internet, home phone, etc

https://en.m.wikipedia.org/wiki/Frontier_Communications

So pretty much an internet provider redirected all traffic to their servers?

OP if you are 100% sure about this you are screwed. No sugarcoating it lol.

eightz - December 25, 2016, 2:38 pm

(Dec 25, 2016 03:33 PM)Purple Kief Wrote: [\[CITE\]](#) So pretty much an internet provider redirected all traffic to their servers?

OP if you are 100% sure about this you are screwed. No sugarcoating it lol.

It could be that they're assisting in an investigation on OP as well.

Ainaj - December 25, 2016, 2:43 pm

(Dec 25, 2016 03:38 PM)eightz Wrote: [\[CITE\]](#) It could be that they're assisting in an investigation on OP as well.

One can only wish

Megabear - December 25, 2016, 2:46 pm

Now this defo does not sound great OP..
take your hdd and destroy it lol.

yotoprules - December 25, 2016, 4:22 pm

Remove any traces of the RAT, delete your VPS account, do a full format of your hard drives to make sure.

QU?CKSILVER - December 25, 2016, 7:58 pm

This is the exact same thing DuckDNS did, but with a twist... Your particular domain was reported as malicious and Dynu was warned about it... Dynu Administrators pointed that domain to one of their endpoints to analyze the traffic coming in. They found out about your domain being used for a botnet, then pointed it back to your original IP address...

Slaves should still connect, unless they managed to uninstall them all for you by using the exact same RAT you're using (which is very unlikely to happen). What a DNS provider would've done is to simply suspend the domain, so that it becomes unresolvable... Just like DuckDNS did to all of us.

Iraqian - December 25, 2016, 11:37 pm

Very interesting!!!

Frontier com is telecommunications and Internet service provider. I work with them most of the time on priv8 duties. That's a real deal as it reached their HQ DPT. I hope you get out if this deal safely. Good luck.

CichyCichoCiemny - December 26, 2016, 1:20 pm

Well, crypt your drives.

?

Sheeple - December 26, 2016, 1:22 pm

(Dec 26, 2016 02:20 PM)CichyCichoCiemny Wrote: [\[CITE\]](#) Well, crypt your drives.

?

encrypting hdds would do nothing, they need to be wiped/destroyed if he's actually going to be in trouble.

Maxie - December 26, 2016, 1:24 pm

Don't crypt your drives. You want to totally format them; writing all 0s to the harddrive. Google for tools.

Avira - December 26, 2016, 2:03 pm

well this thread is bullshit, however, even if it is legit For someone to steal your domain reg account and point it to their own Ip for however long proves nothing, if they wanted you to have no bots they would've kept the domain pointed to their own server anyway

Also, they would have to know exactly what rat you're using otherwise there would be no way for him to issue commands to the infected machines. how about a name? (Of the "researcher")

Katarina Du Couteau - December 26, 2016, 2:05 pm

You are 100% fucked, someone is dedicated in finding you.

RiP

Nickname. - December 26, 2016, 2:42 pm

Well I am sure you got nothing to worry about since the feds wouldnt take your slaves they rather

catch you when you maintain your clients.

cashf - December 29, 2016, 9:22 pm

Just as update:

- All looks pretty safe still (I don't want to elaborate details here, what exactly I did to prevent that the VPS company can get any info about myself, just I think that is was "enough")
- Nothing has been done with the vics. Setup was for a test only.
- VPS suspended my server couple days before. I realized that the RAT connected to the VPS-IP directly. This made the company suspend my VPS. The reason behind this was, that spamhaus listed my VPS IP as C&C server in a blacklist. Obviously they had send an abuse letter to my VPS company which caused them to take down my VPS.
- Disk of the VPS was completely overwritten at this time. Still VPS company took it down due to spamhaus abuse letter. VPS wasn't a bulletproof one.
- Also DNS and a Domain which I used got suspended.

Pretty harsh reaction, I know, anyway I think that the setup was relatively safe.

I think this can be closed now.

Have a great day!

QU?CKSILVER - December 30, 2016, 6:14 am

So Dynu suspended your domain as well?

cashf - December 30, 2016, 6:40 am

(Dec 30, 2016 07:14 AM)QU?CKSILVER Wrote: [\[CITE\]](#) So Dynu suspended your domain as well? Actually not, dynu was/is still standing. But 2 other backup DNS from alternative DNS providers had been gone. Also the VPS got suspended.

Dynu pointed the domain back to my original IP and dynu WAS and IS the last piece in this whole setup that is still standing. Now worthless of course.

Well... strange story, I will not use this dynu DNS from now on...

JoshuTee - December 30, 2016, 7:38 am

Especially when this looks safe, it's best for your safety to uninstall all your clients and nuke your hard drive with DBAN.

It's frankly quite possible that your will get raided. A friend of mine was in a simulator situation and he DID in fact get raided

Armada - December 30, 2016, 9:01 am

Really 3 pages for this?

@OP, your DNS got flagged and they null routed it to a honeypot.

Simple as that.

xtommyxnguyenx - January 25, 2017, 6:14 am

Hey man! That's totally messed up dude but PM your Skype name. I think I got something you might be interested in :D

ImSimplyNameless - January 25, 2017, 6:17 am

(Jan 25, 2017 07:14 AM)xtommyxnguyenx Wrote: [\[CITE\]](#) Hey man! That's totally messed up dude but PM your Skype name. I think I got something you might be interested in :D
You brought up a pretty old thread here

Mohinder - January 25, 2017, 7:21 am

(Jan 25, 2017 07:17 AM)imsimplynameless Wrote: [\[CITE\]](#) You brought up a pretty old thread here
Yeah, this thread is really old. I can't imagine people are talking in a 30-days old thread. WTF is happening these days?

Really?

Armada - January 25, 2017, 5:10 pm

(Jan 25, 2017 07:14 AM)xtommyxnguyenx Wrote: [\[CITE\]](#) Hey man! That's totally messed up dude but PM your Skype name. I think I got something you might be interested in :D

(Jan 25, 2017 07:17 AM)imsimplynameless Wrote: [\[CITE\]](#) You brought up a pretty old thread here

(Jan 25, 2017 08:21 AM)Mohinder Wrote: [\[CITE\]](#) Yeah, this thread is really old. I can't imagine people are talking in a 30-days old thread. WTF is happening these days?

Really?

Stop fawking grave digging, OP already noted this thread should be closed.

Malicious007 - January 25, 2017, 6:23 pm

lol , maybe they like you're bots

FBG Duck - January 25, 2017, 6:24 pm

Dude all you need to do is scan the qbot exploit onto your dark comet

Mohinder - January 26, 2017, 5:17 am

(Jan 25, 2017 06:10 PM)Armada Wrote: [\[CITE\]](#) Stop fawking grave digging, OP already noted this thread should be closed.

How is this post not grave digging x')?