

Forum:[Hack Forums](#)

Thread: [RAT Anonymity \(Misconceptions and Challenge\)](#)

R.I.P - May 19, 2017, 9:49 pm

I've done lots of digging and, according to countless threads, the only universally accepted measure needed to be taken to become anonymous is a VPN.

Others talk about VPS', VM's, SOCKS5 proxies, SSH tunnels, proxy chains, etc. Everyone has an opinion.

Something almost no one has mentioned, which I think is astonishing -- the DNS and payment methods.

When the target reverse engineers the virus and traces you, they'll end up at your DNS. Not your VPN, not your SOCKS5, but your DNS. I know what you're going to say, "but the DNS uses my VPN IP." Well, let's suppose you happened to load the DNS website JUST ONCE without the VPN on. Let's suppose your VPN disconnected for half a second, when you refreshed the DNS page. Now they have your IP, and when the cops come asking them who owns that DNS, wait for a knock on your door.

Hell, let's assume you were perfect and never showed your real IP to the DNS website. What email did you use? Some throwaway hotmail, gmail, or yahoo, I'm sure. And guess what, if you ever logged into that throwaway email, even AGES ago, without a VPN on, the authorities can easily subpoena the owner of the email provider for your IP logs. Screwed.

This works the other way around too. Accidentally kept your VPN on for a quick look at Britney's hawt FB post? Were you auto-logged into your personal Outlook mailbox with your VPN on? Maybe you just kept that Skype/Discord chat opened to send a quick message after connecting? Well, you just gave that VPN an identity.

If you were 100% perfect all this time, better check your Bitcoin account. Yeah, transactions can be traced back to a service, and how are BTC purchased? Often times, via PP and CC. Both identifiers to you. The BTC you sent to the DNS service, the BTC you sent to the VPN service, and the VPS service. All of this can be traced back to you, unless you took precautions here as well.

So forget the VPS, VPN, VM, SOCKS5, TOR, and SSH. That's just what you need to stay afloat. If you want safety, hardened anonymity, you need perfection. Unless you're a faultless machine, you'll need a separate PC. The phrase is, "don't shit where you eat".

If you just use RATs to fool around with adclickers and miners, don't even worry about it. But if you care about anonymity, HARDENED anonymity, you seriously need to run a cost/benefit analysis. It'll take focus, concentration, and time. One slip up and you'll be shoveling snow in a Siberian prison.

Sometimes you can get caught up in setting up and creating and researching and troubleshooting for hours and hours, for a task like RATing, just for what you think is easy money. Take a step back and think, how much could you earn from cleaning out people's pools 3 times a week? I'd say unless you're doing this at least partially for enjoyment, you're wasting your time.

kevy42 - May 20, 2017, 3:29 am

i dont rat, nor have anything setup, but my way would be to get a Windows VPS on an offshore bulletproof/abuse tolerance server, than setup a VPN on a VPS(also on an offshore bullet proof host), and make it so that the Windows server ONLY lets me login with the VPN on.. that way i dont need to mess with DNS's and crap, if the server gets compromised well they wont get my ip, and sence bowth the VPN and VPS is offshore bullet proof.. i dont see anyone being able to with ease. or alternatively il VPN + TOR when logging into the VNC, that way the traffic is encrypted though the TOR exit nodes aswell, making in insanely diffecult for anyone to pin me down.

My method would have flaws.. any method has flaws.. but its alot safer than the usual things ppl do, like using temp mail and forgetting to use the VPN

Rottapotta - May 20, 2017, 6:07 am

You are way too paranoid.

No cop will catch you for ratting, because its just skid shit.

bzr? - May 20, 2017, 6:08 am

Unneeded. Everyone knows this. There are paid services here like Armadas DNS service and PunkDNS to provide this.

Also, if you buy a RAT here with intent for malicious use and use PayPal or another form of easily traceable currency, I hope you get caught.

occupi - May 20, 2017, 6:10 am

(May 20, 2017 06:07 AM)Rottapotta Wrote: [\[CITE\]](#) You are way too paranoid.

No cop will catch you for ratting, because its just skid shit.

That explains why the FBI got involved with Blackshades then, right?

Don't just write off anonymity as inconvenient or paranoid. It does matter.

Mirakuru - May 20, 2017, 7:06 am

(May 20, 2017 06:07 AM)Rottapotta Wrote: [\[CITE\]](#) You are way too paranoid.

No cop will catch you for ratting, because its just skid shit.

It doesn't matter what you are using, crime is crime.

Rottapotta - May 20, 2017, 7:59 am

(May 20, 2017 06:10 AM)occupi Wrote: [\[CITE\]](#) That explains why the FBI got involved with Blackshades then, right?

Don't just write off anonymity as inconvenient or paranoid. It does matter.

(May 20, 2017 07:06 AM)Mirakuru Wrote: [\[CITE\]](#) It doesn't matter what you are using, crime is crime.

OP: Because Blackshades (was meant for illegal purposes) was blatantly being used illegally and it had a plugin that allowed you to display a ransom page. If you really can't keep the DNS hidden from your other shit, such as cookies, cache etc, stop ratting completely.

Mirakuru: Didn't get your point.

Autist - May 20, 2017, 8:33 pm

What I think is the safest way is having a VPN and using a VM and in that vm have it save as slate and in that vm connect to an rdp that you bought with Bitcoin. Can't get any safer than this

R.I.P - May 20, 2017, 10:16 pm

(May 20, 2017 03:29 AM)WeedmasterOG Wrote: [\[CITE\]](#) My method would have flaws.. any method has flaws.. but its alot safer than the usual things ppl do, like using temp mail and forgetting to use the VPN

The method you mentioned is easily the most secure, without being paranoid. Unless you're some high profile hacker using tens of thousands of slaves for highly illegal activity, that is. In that case, a chain of VPNs and secure RDPs would be necessary. In the end though, if you're wanted enough, you'll be found.

(May 20, 2017 06:07 AM)Rottapotta Wrote: [\[CITE\]](#) You are way too paranoid.

No cop will catch you for ratting, because its just skid shit.
"RAT'ing" itself is harmless. It all depends how the RAT is used.

(May 20, 2017 06:08 AM)bzr? Wrote: [\[CITE\]](#) Unneeded. Everyone knows this. There are paid services here like Armadas DNS service and PunkDNS to provide this.

Also, if you buy a RAT here with intent for malicious use and use PayPal or another form of easily traceable currency, I hope you get caught.

If everyone knows this then why are 99% of DNS' No-IP or other public services? I'm not hating on these DNS', just pointing out that they can pose a threat to anonymity for those concerned.

As far as buying RATs goes, you don't put yourself in much risk if you buy a RAT with traceable currency. The RAT itself has no play in how you get caught, unless it is a RAT where slaves are managed by an online service.

Rottapotta - May 21, 2017, 5:12 am

(May 20, 2017 10:16 PM)R.I.P Wrote: [\[CITE\]](#) "RAT'ing" itself is harmless. It all depends how the RAT is used.

If everyone knows this then why are 99% of DNS' No-IP or other public services? I'm not hating on these DNS', just pointing out that they can pose a threat to anonymity for those concerned.

1. People use it as "legal" malware, what did you expect? Obviously you are going to start defend RATting because you do it in an illegal way, no way to talk around it.

2. There's no threat to your anonymity, because they don't do anything against you, unless you use the DNS in a malicious way. Why'd u need that kind of privacy, when your shit wont get leaked either way?

TheWarOwl - May 21, 2017, 6:41 am

There's tons of ways to get caught if you're doing something illegal. Usernames can get you caught, if you have a username or email that you're using elsewhere that they can link to your anonymous persona to your others that you may not have used a vpn on - caught.

Database Hacks - many websites have been hacked and have our real info in it. If they can tie your ip/email/username or anything to what's in a dumped database... you can get caught. Even in backwards order - if you typically go somewhere without a vpn, then go there WITH a vpn, there's a way to tie the two.

Basically - anonymity means paying with different bitcoin address's, only using your vpn when your

using your anonymous identity, separate emails and usernames for your anonymous identity etc... and shitloads of what's called "false info". I've seen people copy the username of someone on the internet they've found that's completely not anonymous, people publicly lie about there location or speak different languages... and the information they give out is always different making it impossible to decipher what's real and what's not. Even just talking about the weather outside is a way people have been located xD lmao

SIM-2053312 - May 21, 2017, 9:00 am

You are a dumbass, you dont even need a VPN to RAT. Thats why HF kids will make no money because they fear being caught each step of the way.

If you think the police will knock on your door for RATing, say goodbye. You dont deserve to have a computer. This is the most stupid shit I ever seen in my life.

Just dont do financial fraud or blackmail and you will have no problems at all.

R.I.P - May 21, 2017, 9:03 pm

(May 21, 2017 05:12 AM)Rottapotta Wrote: [\[CITE\]](#) 1. People use it as "legal" malware, what did you expect? Obviously you are going to start defend RATting because you do it in an illegal way, no way to talk around it.

2. There's no threat to your anonymity, because they don't do anything against you, unless you use the DNS in a malicious way. Why'd u need that kind of privacy, when your shit wont get leaked either way?

1. What do you mean "what did you expect?" The vast majority of HF don't use RATs for "legal," purposes, don't kid yourself. Further, I never "defended RAT'ing". I am saying that it is harmless in itself, it all depends what one does with it.

2. "If they don't do anything against you, there's no threat to your anonymity." Anonymity is independent of what they do to you; the point is that a leaked IP is always a threat to your anonymity, whether or not you're using the DNS for malicious purposes.

(May 21, 2017 09:00 AM)Chef Curry Wrote: [\[CITE\]](#) You are a dumbass, you dont even need a VPN to RAT. Thats why HF kids will make no money because they fear being caught each step of the way.

If you think the police will knock on your door for RATing, say goodbye. You dont deserve to have a computer. This is the most stupid shit I ever seen in my life.

Just dont do financial fraud or blackmail and you will have no problems at all.

HF kids will make no money because of being cautious? Nah, at worst all they'll do is waste some time being overly paranoid. If you ask me, it's better to waste some time than to risk losing your future, no matter how small the chances of that happening are.

You're ignorant if you think RAT'ing can't ever become illegal enough to cause a police raid. Do you have any idea what kind of activity can be done with full access to someone's PC? I'm not going to start listing examples, but if you can't think of at least a dozen things you have no idea what you're talking about.

There's way more than financial fraud and blackmail that can warrant investigation. You listed these two categories yourself as two things that can land someone in prison. RAT'ing itself no, but for the third time it depends what one does with the RAT.

Mr JOkeR - May 22, 2017, 3:05 am

It's easy AF.

RAT From OFF-Shore VPS/RDP .

You're 100% secure .

R.I.P - May 22, 2017, 3:06 am

(May 22, 2017 03:05 AM)Mr JOkeR Wrote: [\[CITE\]](#) It's easy AF.

RAT From OFF-Shore VPS/RDP .

You're 100% secure .

It seems like a good idea but there is always the risk that the RDP/VPS goes out of service, and then your RAT and all your clients go to nothing.

Armada - May 22, 2017, 9:19 pm

VPN in to an RDP Server you Setup and run everything from there.

Problem solved.....?

Wait that was too easy. ?

Armada - May 22, 2017, 10:39 pm

(May 22, 2017 10:14 PM)Friedrich Nietzsche Wrote: [\[CITE\]](#) No real reason to use an RDP and a VPN unless your VPN provider is one that will snitch on you. If you can buy an RDP, why not just set up an OpenVPN server on it and clear logs every few days?

Believe you failed to see OPs paranoia.

However, I tend to agree, it's more routing and HOPs than I want to route my traffic through if I can avoid to do so....

R.I.P - May 22, 2017, 11:03 pm

(May 22, 2017 10:42 PM)Friedrich Nietzsche Wrote: [\[CITE\]](#) I know OP is paranoid, just pointing out that it was still a little too much for the average HF RATters.

I'm not paranoid because I don't run a RAT.

I wanted to make this topic to hopefully shed some light on just how difficult it is to be anonymous, and some pitfalls people don't talk about.

Armada - May 22, 2017, 11:15 pm

(May 22, 2017 11:03 PM)R.I.P Wrote: [\[CITE\]](#) I'm not paranoid because I don't run a RAT.

I wanted to make this topic to hopefully shed some light on just how difficult it is to be anonymous, and some pitfalls people don't talk about.

Not difficult at all, just know your routing and processing.... :)

R.I.P - May 22, 2017, 11:19 pm

(May 22, 2017 11:15 PM)Armada Wrote: [\[CITE\]](#) Not difficult at all, just know your routing and processing.... :)

Use a VPN on the original machine, and connect to the RDP through the VPN, is what you're saying?

The issue then would be finding the right RDP. Among the available RDPs, there are a select few that allow the type of abuse users will be using them for. Among those, even fewer will keep anonymity in mind (no logging), and among those, even fewer will be affordable.

Even an RDP that meets all those criteria would need to stay alive for a long time, else all the work

done on that RDP is lost. Setting up one's own RDP is the only way to go about it, but that's useless because the whole point of setting up an RDP is for anonymity, and setting up one's own RDP (presumably, in one's own location) defeats that purpose.

Armada - May 22, 2017, 11:21 pm

(May 22, 2017 11:19 PM)R.I.P Wrote: [\[CITE\]](#) Use a VPN on the original machine, and connect to the RDP through the VPN, is what you're saying?

The issue then would be finding the right RDP. Among the available RDPs, there are a select few that allow the type of abuse users will be using them for. Among those, even fewer will keep anonymity in mind (no logging), and among those, even fewer will be affordable.

Even an RDP that meets all those criteria would need to stay alive for a long time, else all the work done on that RDP is lost. Setting up one's own RDP is the only way to go about it, but that's useless because the whole point of setting up an RDP is for anonymity, and setting up one's own RDP (presumably, in one's own location) defeats that purpose.

Cayman Islands. Nuff said.

R.I.P - May 22, 2017, 11:26 pm

(May 22, 2017 11:21 PM)Armada Wrote: [\[CITE\]](#) Cayman Islands. Nuff said.

Book flight to Cayman Islands --> Set up PC --> Set up RDP software --> Leave --> ??? --> Profit

something like this I presume

Armada - May 22, 2017, 11:27 pm

(May 22, 2017 11:26 PM)R.I.P Wrote: [\[CITE\]](#) Book flight to Cayman Islands --> Set up PC --> Set up RDP software --> Leave --> ??? --> Profit

something like this I presume

Well I guess, I just ordered my shit online, but if you wanna vacation in the process sure. LOL

SIM-2053312 - May 23, 2017, 6:13 am

(May 21, 2017 09:03 PM)R.I.P Wrote: [\[CITE\]](#) 1. What do you mean "what did you expect?" The vast majority of HF don't use RATs for "legal," purposes, don't kid yourself. Further, I never "defended RAT'ing". I am saying that it is harmless in itself, it all depends what one does with it.

2. "If they don't do anything against you, there's no threat to your anonymity." Anonymity is independent of what they do to you; the point is that a leaked IP is always a threat to your anonymity, whether or not you're using the DNS for malicious purposes.

HF kids will make no money because of being cautious? Nah, at worst all they'll do is waste some time being overly paranoid. If you ask me, it's better to waste some time than to risk losing your future, no matter how small the chances of that happening are.

You're ignorant if you think RAT'ing can't ever become illegal enough to cause a police raid. Do you have any idea what kind of activity can be done with full access to someone's PC? I'm not going to start listing examples, but if you can't think of at least a dozen things you have no idea what you're talking about.

There's way more than financial fraud and blackmail that can warrant investigation. You listed these two categories yourself as two things that can land someone in prison. RAT'ing itself no, but for the third time it depends what one does with the RAT.

No shit sherlock. I know tons of ways of how someone can land into prison but usually these two are the biggest. Others are extremely rare lol or not worth doing due to risks, if it doesn't make someone money then why do it?

Rottapotta - May 23, 2017, 7:39 am

(May 21, 2017 09:03 PM)R.I.P Wrote: [\[CITE\]](#) 1. What do you mean "what did you expect?" The vast majority of HF don't use RATs for "legal," purposes, don't kid yourself. Further, I never "defended RAT'ing". I am saying that it is harmless in itself, it all depends what one does with it.

2. "If they don't do anything against you, there's no threat to your anonymity." Anonymity is independent of what they do to you; the point is that a leaked IP is always a threat to your anonymity, whether or not you're using the DNS for malicious purposes.

HF kids will make no money because of being cautious? Nah, at worst all they'll do is waste some time being overly paranoid. If you ask me, it's better to waste some time than to risk losing your future, no matter how small the chances of that happening are.

You're ignorant if you think RAT'ing can't ever become illegal enough to cause a police raid. Do you have any idea what kind of activity can be done with full access to someone's PC? I'm not going to start listing examples, but if you can't think of at least a dozen things you have no idea what you're talking about.

There's way more than financial fraud and blackmail that can warrant investigation. You listed these two categories yourself as two things that can land someone in prison. RAT'ing itself no, but for the third time it depends what one does with the RAT.

1. I mean that RATting is considered a malicious activity, and that 99.99% of HF's users are using it for malicious activities. By calling it harmless you of course are defending it.

2. If LE deals with all the HF kids who use their home connection for RATting we would see an epidemic of 9 years old in prison. A huge amount of RAT samples use home connection, and you would know if you just bothered downloading and analyzing some samples from hybrid-analysis.

R.I.P - May 23, 2017, 9:43 am

(May 23, 2017 07:39 AM)Rottapotta Wrote: [\[CITE\]](#) 1. I mean that RATting is considered a malicious activity, and that 99.99% of HF's users are using it for malicious activities. By calling it harmless you of course are defending it.

2. If LE deals with all the HF kids who use their home connection for RATting we would see an epidemic of 9 years old in prison. A huge amount of RAT samples use home connection, and you would know if you just bothered downloading and analyzing some samples from hybrid-analysis.

1. RAT'ing is not a malicious activity in and of itself. It is a Remote Administration Tool, and is used for legit purposes as well. Just because 99.99% of HF uses it maliciously does not make it a malicious tool. That's like saying a fork is a malicious tool because it can be used to stab someone.

2. Those HF kids who use their home connections for RAT'ing aren't doing anything LE would care about. CD drive spam doesn't get anyone's attention -- blackmail and fraud does.

Rottapotta - May 23, 2017, 10:00 am

(May 23, 2017 09:43 AM)R.I.P Wrote: [\[CITE\]](#) 1. RAT'ing is not a malicious activity in and of itself. It is a Remote Administration Tool, and is used for legit purposes as well. Just because 99.99% of HF uses it maliciously does not make it a malicious tool. That's like saying a fork is a malicious tool because it can be used to stab someone.

2. Those HF kids who use their home connections for RAT'ing aren't doing anything LE would care about. CD drive spam doesn't get anyone's attention -- blackmail and fraud does.

1. However when anonymity is required, it is 100% malicious. Why would someone need to silently install a RAT while being behind 90 proxies and 7 VPNs if they are using it to monitor their kid's computer? I believe a more reasonable comparison would be to how a machine gun is considered a malicious weapon and not one used for self defense.

2. If you are doing blackmail and fraud then you would not use a RAT, you would use a proper banking botnet (namely Panda, Tinba, TinyNuke, and other players on the market) bullshit

Armada - May 23, 2017, 11:50 am

(May 23, 2017 10:00 AM)Rottapotta Wrote: [\[CITE\]](#) 1. However when anonymity is required, it is 100% malicious. Why would someone need to silently install a RAT while being behind 90 proxies and 7 VPNs if they are using it to monitor their kid's computer? I believe a more reasonable comparison would be to how a machine gun is considered a malicious weapon and not one used for self defense.

2. If you are doing blackmail and fraud then you would not use a RAT, you would use a proper banking botnet (namely Panda, Tinba, TinyNuke, and other players on the market) bullshit

First off, your stupid, but secondly and more pressing on my cranium is how the hell you've not been closed yet... lol

I mean you literally just recommended a bunch of banking malware to another user, which is a direct violation of the site rules. And you do this constantly. I am astounded your still allowed to login man. be more careful with what you recommend.

Rottapotta - May 23, 2017, 11:55 am

(May 23, 2017 11:50 AM)Armada Wrote: [\[CITE\]](#) First off, your stupid, but secondly and more pressing on my cranium is how the hell you've not been closed yet... lol

I mean you literally just recommended a bunch of banking malware to another user, which is a direct violation of the site rules. And you do this constantly. I am astounded your still allowed to login man. be more careful with what you recommend.

I never recommended, I said a list of botnets/banking trojans that are made for malicious usage.

Fun to see that you call me stupid when you dont even know proper grammar.

Kisame? - May 23, 2017, 11:57 am

(May 23, 2017 11:50 AM)Armada Wrote: [\[CITE\]](#) First off, your stupid, but secondly and more pressing on my cranium is how the hell you've not been closed yet... lol

I mean you literally just recommended a bunch of banking malware to another user, which is a direct violation of the site rules. And you do this constantly. I am astounded your still allowed to login man. be more careful with what you recommend.

You're* stupid.

Ontopic: If you want to RAT "safely", I'd recommend you create a proper setup. Work from an offshore, bulletproof VPS, to which you only connect with an offshore VPN which doesn't log a thing. The best thing is to configure the VPN in your router. I haven't done this myself, as I think it might be a bit over the top (for me, atleast), but if you do it properly, no traffic will be allowed over your normal connection. This means your VPN can't "drop for a second" and give you away.

Do not use any identities that could be linked to your real one somehow. Use secure services (for mail, I think creating a protonmail on the VPS we've just talked about would be a good idea).

Encrypt your HDD with VeraCrypt if you'd like, use a daisy chain of proxies/VPN's, only buy a DNS hosted by a company that doesn't give out any info nor gives a fuck about anything you do with it...

Set up your browser properly, spoof the user-agent, disable WebRTC, etc.
Make sure your real DNS or IPv6 isn't leaking through ...

If you know what you're doing, and actually have a setup which is done professionally, using only high-quality services, then you can be (almost) fully anonymous. It's just a matter of effort and knowledge.

Armada - May 23, 2017, 12:02 pm

(May 23, 2017 11:55 AM)Rottapotta Wrote: [\[CITE\]](#) I never recommended, I said a list of botnets/banking trojans that are made for malicious usage.

Fun to see that you call me stupid when you dont even know proper grammar.
Do not recommend or even SUGGEST banking malware around here man.

Its your account that can be lost/closed. Its for your OWN good.

But sure, lets rip on my grammatical errors instead of listening to logic. ?

Rottapotta - May 23, 2017, 12:05 pm

(May 23, 2017 12:02 PM)Armada Wrote: [\[CITE\]](#) Do not recommend or even SUGGEST banking malware around here man.

Its your account that can be lost/closed. Its for your OWN good.

But sure, lets rip on my grammatical errors instead of listening to logic. ?
I made examples, not suggestions.

Your post had absolutely no logic in it.

Now stay on-topic.

Armada - May 23, 2017, 12:07 pm

(May 23, 2017 12:05 PM)Rottapotta Wrote: [\[CITE\]](#) I made examples, not suggestions.

Your post had absolutely no logic in it.

Now stay on-topic.
Whatever, don't listen to me, enjoy the sanctions I am sure you will eventually receive.

Have fun with your thread and topic, I will just bow the fuck out now, because obviously no one cares about experienced opinion anymore. That has become very clear in the last few months to me.

Kisame? - May 23, 2017, 12:18 pm

(May 23, 2017 12:05 PM)Rottapotta Wrote: [\[CITE\]](#) I made examples, not suggestions.

Your post had absolutely no logic in it.

Now stay on-topic.

Talking about banking bots is enough to get your account closed. I'd listen to Armada's advice here... Or don't, why should I give a flying fuck

R.I.P - May 24, 2017, 8:24 am

(May 23, 2017 10:00 AM)Rottapotta Wrote: [\[CITE\]](#) 1. However when anonymity is required, it is 100% malicious. Why would someone need to silently install a RAT while being behind 90 proxies and 7 VPNs if they are using it to monitor their kid's computer? I believe a more reasonable comparison would be to how a machine gun is considered a malicious weapon and not one used for self defense.

2. If you are doing blackmail and fraud then you would not use a RAT, you would use a proper banking botnet (namely Panda, Tinba, TinyNuke, and other players on the market) bullshit

1. Anonymity does not presuppose maliciousness. There are many reasons to stay anonymous. For example, one may want to stay anonymous because giving up one's identity and IP address to a random client on one's RAT could pose a security risk. Yes, even if that client is willingly receiving help through a RAT, it is a security risk.

2. Now you're assuming that no one uses RATs for blackmail, fraud, and other highly illegal activity. That's obviously false.

(May 23, 2017 11:57 AM)David? ?Gilmour Wrote: [\[CITE\]](#) Work from an offshore, bulletproof VPS, to which you only connect with an offshore VPN which doesn't log a thing[...]

only buy a DNS hosted by a company that doesn't give out any info nor gives a fuck about anything you do with it...

These are the keys. However, there is no such thing as a truly "bulletproof" VPS, and the closer you can get to one the more expensive the price goes up. VPNs are forced to log a minimum of information for simple functionality, but I would say finding a VPN that doesn't log a thing is easier than a VPS.

A DNS company that doesn't care on the other hand... Any DNS company would comply if they receive an email from the feds. But why would you need a DNS if you have a bulletproof VPS?

FeeliNx - May 27, 2017, 8:28 am

thank you for posting OP, reading what people posting here and thinking of my anonymity level again.... stay safe everyone!

TheWarOwl - May 27, 2017, 10:17 am

Rule #1 of life: don't break the law

Rule #2 of life: if you break the law, do your homework first