

Forum:[Hack Forums](#)

Thread: [Ultimate Doxing - Ep. 7 - VPN Doxing](#)

?Criminal - September 10, 2016, 3:09 pm

Haven't done one of these in awhile so figured i'd release something helpful for my fellow PI's in the community, alot of us probably come to the point in our investigations where we stumble upon a VPN IP and usually consider it a dead end but a good PI always thinks outside the box to turn a dead end into a new lead.

Here are some techniques you can use to identify people behind VPN IP's:

Technique 1. Se'ing the VPN provider directly

Im not gonna spoonfeed and go indepth into this but the jist of it is to email them scare tactics this could involve using fancy legal lingo or fabricated documents without going into too much detail. Now as some of you may know some VPN's don't log anything but all VPN's keep billing logs/sign up logs so you could still possibly get a home IP on someone even if the VPN server directly doesn't store logs but the web server where you manage your account does.It's also possible to use LE related pretexts but I will not get into that because it's risky to use those.Another thing is to keep in mind is if you try to use this method to dox a shared IP which 100's of people use, you will need timestamps along with the IP so they can see which user was using it at the time.Heres an old thread I found of the user killerpop who managed to do this:

<https://hackforums.net/showthread.php?tid=1967070> as you can see emailing vpn providers can prove useful in your work on finding people.

Technique 2. Tricking the person using the VPN directly

One trick even I managed to succumb too my self in the past was some vpns have ip login history so if you message the person "oh hey use my vpn login it's way better then that vpn your using" you can have them log in change the pass kick them off and check the IP login history for their home connection, this method is extremely potent because almost anyone can fall for it when there off their guard I my self fell for it not realizing what the attacker was trying to do at first.This is just an example pretext im sure theres other interesting ways to get home connections.

Technique 3. Client Side Channel Attacks such as Cache Timing Attacks

if people order food online or visit sites that involve geolocation like if people travel alot and have viewed their own address on google maps to check for directions for example to travel somewhere and back, you can use javascript timing side channel attacks to get their city and state, if they used craigslist sometimes it shows the subdomain of the city there in so thats another site you can use a timing attack on to get city information from, timing attacks are deadly because they completely disregard whether your using a VPN or not and most timing attacks by design will always work only some deadly ones like the pixel perfect attack that was shown off at an old defcon were fixed.Most of this info gets stored in your browsers cache or browser history so it's something to keep in mind.This will only work if the person using the VPN previously cached info related to their city and state in the browser they use.Theres tons of academic research papers you can find on google to get an idea on how to set up the malicious javascript.

Technique 4. Using super convincing bait to force them off the VPN

This one is pretty easy to get creative with, one can get a dummy domain and host a convincing file such as [example.com/usersalias-criminal-complaint.pdf](#) and you mention to them it shows how the feds got all there emails and IP's and by instilling worry and fear they will try extremely hard to view this fake document even going as far as switching their vpn off for a bit, iv'e used this method at

least twice and it's a very high success rate. Make sure to set up apache/nginx rules to ensure it serves a 403 forbidden page if there on the VPN. It could be a normal page too if you don't want to use a PDF like I said being creative is key for this one. From there you can ISP dox the home connection or grep DB's for it to gain further info.

Technique 5. Grepping alias/emails in DB's

Sometimes you can find old home IP's from their emails and aliases directly sidestepping the need to even deal with the VPN IP in the first place, this requires a large private db collection if you don't want to rely on leakedsource which despite having 2 billion entries sometimes falls short and can't get the info you desire on your target.

Technique 6. VPN Correlation Attacks

Sites like skypegrab allow you to find skype ID's linked to a single VPN IP because a lot of skypes were resolved and by doing this you may be able to find a person's multiple aliases, possibly a home IP if one of their skypes had a home IP resolved for it before they used the VPN so VPN IP's could be very useful to an attacker in some scenarios.

Technique 7. VPN Pattern Correlation Attacks

Similar to the previous technique sometimes people use the same VPN provider based on the ASN ranges so you can sometimes identify a person just based on the VPN they use, this combined with voice prints (A lot of people will use a mic while using a VPN so voiceprints are usually obtainable most of the time) and other metadata can really nail someone's head to a cross.

Technique 8. Disconnection VPN Correlation Attacks

This attack while deadly is very tricky to pull off without an automated script for it, you need to find a platform that they use such as jabber or skype and you want to ddos a bunch of home IP's you think is theirs. You can do this manually but it can take ages, you'd have to make an excel graph of every IP you hit and keep logs of that but once you know you hit the right IP their jabber will go off or their skype will go off, this allows you to identify their home connection completely side-stepping their VPN. If you really want to identify someone bad enough and other techniques failed this is the way to go.

Technique 9. Clickjacking Attacks

Not many people may know this but clickjacking has been used for awhile to deanonymize people. VPN's don't matter in a clickjacking attack because if the victims are on an account with real PII a VPN won't prevent info disclosure happening this way, common ways include getting the person's twitter profile or facebook profile and getting names, DOB and other info from them.

Technique 10. Targeted Malware

If you can get malware installed on the person's comp you can force the person to make outbound connections with their home connection by killing the openvpn.exe process. This is by far my most favorite and sneakiest way to get home connections. Malware is pretty much game over most of the time VPN or not.

I hope you guys enjoyed this thread and now realize VPN's can be thwarted if you put the effort in.

Motiv - September 10, 2016, 3:12 pm

I wish you'd make this private haha. This is absolutely amazing, and I've never seen a member give out so many methods like this. You're a genius.

TheTwitchTerror - September 10, 2016, 4:46 pm

Great methods criminal well done

Light. - September 10, 2016, 9:47 pm

unless you're dealing with a retard that has no opsec common sense this isn't going to work lol se info off of pia or mullvad and I'll eat my words

Description - September 10, 2016, 9:53 pm

Your tuts are always super good and interesting.

Thanks for sharing.

?Criminal - September 10, 2016, 10:05 pm

(Sep 10, 2016 09:47 PM)Light. Wrote: [\[CITE\]](#) unless you're dealing with a retard that has no opsec common sense this isn't going to work lol se info off of pia or mullvad and I'll eat my words mullvad doesn't even have a proper login system(they use acc numbers) they don't store info period and PIA even if you faked LE they wouldn't give anything anyways if your gonna use method 1 my as well try a VPN thats actually known to give info out like [censored] and the other methods work perfectly fine not everyones gonna think about all this 24/7 people slip up especially the login history trick so many people have been gotten with that.Method 1 the only people I seen aside from killerp0p pull it off with evidence is mr robot I seen him mention it once so chances are he got info from a VPN provider by emailing them before, the methods been done before it's not impossible if thats what you think but I never implied or said it works on every vpn provider either it's just an option to try.

Toby Flenderson - September 10, 2016, 10:07 pm

round of applause! thanks for the info bro!

Agonises - September 10, 2016, 11:56 pm

To be honest some of these methods don't work, considering the anonymity and protection VPN provides for their uses strengthen. Such as:

"Now as some of you may know some VPN's don't log anything but all VPN's keep billing logs/sign up logs so you could still possibly get a home IP on someone even if the VPN server directly doesn't store logs but the web server where you manage your account does."

People who are smart enough tend to use another temporary VPN, or even route their traffic through tor to purchase a VPN Subscription and would use a throw-away email, at least that's what I did. Furthermore "so you could still possibly get a home IP" , if you get a HOME IP that's dynamic, the use of that is minimal to the average doxer.

Technique 2 seems like such a flawed idea that most probably will never work. If it works then the person is retarded and you could easily grab his IP Address (Which is most probably what this thread is aimed at, getting the real ip behind the VPN).

Technique 3 requires you to contact the recipient. Of which may or may not work.

Technique 4 sounds really ridiculous and non-believable in my eyes, if you're trying to send them a file you might as well try to rat them. But then again a few of these methods require the recipient to be somewhat stupid.

Technique 5 has nothing to do with VPN IPs.

Technique 6 works, and has worked for me in the past. Good job on pointing that one out.

Technique 7 relies on the other person to be stupid and use the same constant Location and doesn't switch regularly. Furthermore "you can sometimes identify a person just based on the VPN they use" I'm sure if you've done background information lookups you'd of already identified the person's online alias (since the normal individual doesn't tend to have great anonymity).

Technique 8 would work especially with DEOB constantly hitting the inbound connection. However since VPNs are advancing, things such as "kill switches" will make it near-impossible to attain a real ip address behind the home connection.

This isn't a reply to argue with you, more to give criticism. You've pointed out a few good methods however the majority seem trash and could "potentially" work.

Light. - September 11, 2016, 12:02 pm

(Sep 10, 2016 11:56 PM)Agonises Wrote: [\[CITE\]](#) To be honest some of these methods don't work, considering the anonymity and protection VPN provides for their uses strengthen. Such as:

"Now as some of you may know some VPN's don't log anything but all VPN's keep billing logs/sign up logs so you could still possibly get a home IP on someone even if the VPN server directly doesn't store logs but the web server where you manage your account does."

People who are smart enough tend to use another temporary VPN, or even route their traffic through tor to purchase a VPN Subscription and would use a throw-away email, at least that's what I did. Furthermore "so you could still possibly get a home IP" , if you get a HOME IP that's dynamic, the use of that is minimal to the average doxer.

Technique 2 seems like such a flawed idea that most probably will never work. If it works then the person is retarded and you could easily grab his IP Address (Which is most probably what this thread is aimed at, getting the real ip behind the VPN).

Technique 3 requires you to contact the recipient. Of which may or may not work.

Technique 4 sounds really ridiculous and non-believable in my eyes, if you're trying to send them a file you might as well try to rat them. But then again a few of these methods require the recipient to be somewhat stupid.

Technique 5 has nothing to do with VPN IPs.

Technique 6 works, and has worked for me in the past. Good job on pointing that one out.

Technique 7 relies on the other person to be stupid and use the same constant Location and doesn't switch regularly. Furthermore "you can sometimes identify a person just based on the VPN they use" I'm sure if you've done background information lookups you'd of already identified the person's online alias (since the normal individual doesn't tend to have great anonymity).

Technique 8 would work especially with DEOB constantly hitting the inbound connection. However since VPNs are advancing, things such as "kill switches" will make it near-impossible to attain a real ip address behind the home connection.

This isn't a reply to argue with you, more to give criticism. You've pointed out a few good methods however the majority seem trash and could "potentially" work.

VPN providers can see your home ip every time you connect to it signing up via tor has no relevance

libc - September 11, 2016, 1:35 pm

(Sep 11, 2016 12:02 PM)Light. Wrote: [\[CITE\]](#) VPN providers can see your home ip every time you connect to it signing up via tor has no relevance

Correct. However, I wouldn't say that signing up via Tor is pointless.

skelly76 - September 11, 2016, 2:24 pm

Great information OP, very useful methods.

Agonises - September 11, 2016, 11:15 pm

(Sep 11, 2016 12:02 PM)Light. Wrote: [\[CITE\]](#) VPN providers can see your home ip every time you connect to it signing up via tor has no relevance

(Sep 11, 2016 01:35 PM)libc Wrote: [\[CITE\]](#) Correct. However, I wouldn't say that signing up via Tor is pointless.

Regarding signing up via tor, I was talking about initial phase of registering. As registering without any form of anonymity can leave you vulnerable to your Home connection IP Address being obtained, such as a MITM attack.

libc - September 12, 2016, 3:17 pm

(Sep 11, 2016 11:15 PM)Agonises Wrote: [\[CITE\]](#) Regarding signing up via tor, I was talking about initial phase of registering. As registering without any form of anonymity can leave you vulnerable to your Home connection IP Address being obtained, such as a MITM attack.

The owners of the VPN can see your IP address every time you connect regardless.

But, of course, signing up through Tor makes finding your IP address a little bit harder on their end, since doing so won't be as simple as viewing the registration IP in the customer database.

Also, looking over customer registration records in a database is not a [MITM attack](#).

Agonises - September 13, 2016, 9:21 am

(Sep 12, 2016 03:17 PM)libc Wrote: [\[CITE\]](#) The owners of the VPN can see your IP address every time you connect regardless.

But, of course, signing up through Tor makes finding your IP address a little bit harder on their end, since doing so won't be as simple as viewing the registration IP in the customer database.

Also, looking over customer registration records in a database is not a [MITM attack](#).

Yes I am aware that everytime you establish a connection the owners of the VPN can see your ip address. I wasn't saying looking over customer registration records in a database is a MITM attack, I'm saying you could be affected in a MITM attack which is why having extra anonymity precautions could help prevent your HOME Ip address being leaked (which is what you purchase a VPN to do, to hide your home Ip address)

e_eoke - September 21, 2016, 11:19 am

Looks like a really nice guide just from browsing it quick, will comment to save for later!

Djehuty - September 21, 2016, 1:41 pm

Don't forget webRTC, most people don't have it properly disabled in the settings of their browser and I get quite a few people using it.

?Criminal - September 21, 2016, 1:43 pm

(Sep 21, 2016 01:41 PM)Djehuty Wrote: [\[CITE\]](#) Don't forget webRTC, most people don't have it properly disabled in the settings of their browser and I get quite a few people using it.

Didn't include it because most premium vpns are protected against it, unless your on like hotspot or

[censored], webrtc is essentially not effective anymore but these methods will always be effective especially the SE ones.

Max P™ - *September 21, 2016, 3:20 pm*

Very interesting. A good amount of information I haven't seen before here. Thanks for sharing!

daku01 - *September 23, 2016, 11:26 am*

Good job.Thanks for sharing...

Regards