

Forum:[Hack Forums](#)

Thread: [Few questions about complete anonymity](#)

pennmw - July 25, 2016, 11:01 am

Hello,

i would like to remain completely anonymous and i have few questions. Let's say i will get a pre-paid internet card, new modem (to not get linked via IMEI number), new laptop (to not get linked by any MAC or HWID number, or any sort of data which are pretty unique for every laptop).

Now, if some website will keep IP logs, is it possible to track me down? Let's say that gov agency (like FBI or whatever) will get that IP logs - can they track me down if laptop / sim card is not being used anymore? In other words, if you have IP of the user which logged to the website 1 month ago, can you track down what was his location 1 month ago at the moment when he was logging in?

Can i find some professional tutorials / guides on HF about complete anonymity?

Regards

Enzio - July 25, 2016, 11:04 am

"In other words, if you have IP of the user which logged to the website 1 month ago, can you track down what was his location 1 month ago at the moment when he was logging in?"

Yes, you can.

pennmw - July 25, 2016, 11:08 am

I just want to assure, do you know that i am talking about pre-paid SIM card, not the normal cable-provided internet by ISP.?

Enzio - July 25, 2016, 11:15 am

(Jul 25, 2016 11:08 AM)pennmw Wrote: [\[CITE\]](#) I just want to assure, do you know that i am talking about pre-paid SIM card, not the normal cable-provided internet by ISP.?

Oh pre-paid? I'm not 100% sure.

vigilante.pw - July 31, 2016, 8:24 am

At the end of the day, if law enforcement with high-end technology and a lot of power wants to find you, the odds are that they will find you. It's probably impossible to be 100% anonymous, so keep that in mind. Having said that, there are a lot of steps you can take to hide from the majority of people (especially people trying to dox you). The steps you mentioned in your thread are steps in the right direction, but keep in mind to think before you do anything that may leak your personal information anywhere. It's important to realize that OPSEC is a mindset, and not just something you do once or twice to clean up months/years of sloppiness. If you need any more help, PM me.

?hoenix - July 31, 2016, 9:24 am

(Jul 31, 2016 08:24 AM)vigilante.pw Wrote: [\[CITE\]](#) At the end of the day, if law enforcement with high-end technology and a lot of power wants to find you, the odds are that they will find you. It's probably impossible to be 100% anonymous, so keep that in mind. Having said that, there are a lot of steps you can take to hide from the majority of people (especially people trying to dox you). The steps you mentioned in your thread are steps in the right direction, but keep in mind to think before you do anything that may leak your personal information anywhere. It's important to realize that

OPSEC is a mindset, and not just something you do once or twice to clean up months/years of sloppiness. If you need any more help, PM me. It's funny seeing you here Keen. ?

vigilante.pw - July 31, 2016, 11:39 am

(Jul 31, 2016 09:24 AM)Veilios Wrote: [\[CITE\]](#) It's funny seeing you here Keen. ?My apologies but who are you? I probably know you under a different alias.

Nerdi - July 31, 2016, 11:42 am

(Jul 25, 2016 11:01 AM)pennmw Wrote: [\[CITE\]](#) Hello,
i would like to remain completely anonymous and i have few questions. Let's say i will get a pre-paid internet card, new modem (to not get linked via IMEI number), new laptop (to not get linked by any MAC or HWID number, or any sort of data which are pretty unique for every laptop).

Now, if some website will keep IP logs, is it possible to track me down? Let's say that gov agency (like FBI or whatever) will get that IP logs - can they track me down if laptop / sim card is not being used anymore? In other words, if you have IP of the user which logged to the website 1 month ago, can you track down what was his location 1 month ago at the moment when he was logging in?

Can i find some professional tutorials / guides on HF about complete anonymity?

Regards

I don't know this for a fact, but I wouldn't be surprised if ISPs kept records of who they assigned IPs to, and when. That way the gov would be able to contact the ISP and figure out who was using a specific IP during a certain time, and they may even be able to dig up more detailed records about your internet history... So nah, I don't think it's easy to be 100% anonymous as there are a LOT of different ways for the gov / ISP to figure out who you are, where you are, etc.

?Criminal - July 31, 2016, 3:15 pm

(Jul 31, 2016 11:42 AM)Nerdi Wrote: [\[CITE\]](#) I don't know this for a fact, but I wouldn't be surprised if ISPs kept records of who they assigned IPs to, and when. That way the gov would be able to contact the ISP and figure out who was using a specific IP during a certain time, and they may even be able to dig up more detailed records about your internet history... So nah, I don't think it's easy to be 100% anonymous as there are a LOT of different ways for the gov / ISP to figure out who you are, where you are, etc.

they do, this is known as DHCP assignment logs or PPOE assignment logs depends if your targets using DSL or cable/optic fiber and yes it is possible to dox people with a few months old IP if you wait too long these logs get cleared however.

(Jul 31, 2016 08:24 AM)vigilante.pw Wrote: [\[CITE\]](#) At the end of the day, if law enforcement with high-end technology and a lot of power wants to find you, the odds are that they will find you. It's probably impossible to be 100% anonymous, so keep that in mind. Having said that, there are a lot of steps you can take to hide from the majority of people (especially people trying to dox you). The steps you mentioned in your thread are steps in the right direction, but keep in mind to think before you do anything that may leak your personal information anywhere. It's important to realize that OPSEC is a mindset, and not just something you do once or twice to clean up months/years of sloppiness. If you need any more help, PM me.

With a hardened setup that comes close to nachashes you can maintain 90% the other 10% that is left out would be opsec slips, correlation/pattern attacks, deanonymized by side channel attacks or Odays and getting lured into a well thought out honeypot.

Pharaoh1100 - July 31, 2016, 3:38 pm

(Jul 31, 2016 03:15 PM)?Criminal Wrote: [\[CITE\]](#) With a hardened setup that comes close to nachashes you can maintain 90% the other 10% that is left out would be opsec slips,

correlation/pattern attacks, deanonymized by side channel attacks or Odays and getting lured into a well thought out honeypot.

And it comes to conclusion that the person is actually flawing himself, and not that "Security is a myth" saying

vigilante.pw - July 31, 2016, 3:43 pm

(Jul 31, 2016 03:15 PM)?Criminal Wrote: [\[CITE\]](#) With a hardened setup that comes close to nachashes you can maintain 90% the other 10% that is left out would be opsec slips, correlation/pattern attacks, deanonymized by side channel attacks or Odays and getting lured into a well thought out honeypot. I more or less agree with you, but there are other things to consider as well. For example, everybody discusses using a privacy-orientated operating system in order to reduce your chances of getting caught or unmasked for whatever you do, but not many people consider that the hardware you use could also be a risk to your OPSEC. My point is that there are a lot of factors to consider, and so it would be foolish to say that you can be 100% anonymous and secure by following a few steps. However, as you have correctly stated, there are definitely things you can do to keep yourself relatively safe from the majority of people.

(Jul 31, 2016 03:38 PM)Pharaoh1100 Wrote: [\[CITE\]](#) And it comes to conclusion that the person is actually flawing himself, and not that "Security is a myth" saying If this was directed at me, read my last post. I'm not saying that there's no point of being mindful about your OPSEC and following security practices - in fact I definitely believe that you should do these things, but it is extremely foolish, arrogant and ignorant to think that you can be 100% secure when pretty much everything the average person uses regarding technology is not made by them.

libc - July 31, 2016, 4:20 pm

(Jul 31, 2016 03:43 PM)vigilante.pw Wrote: [\[CITE\]](#) I more or less agree with you, but there are other things to consider as well. For example, everybody discusses using a privacy-orientated operating system in order to reduce your chances of getting caught or unmasked for whatever you do, but not many people consider that the hardware you use could also be a risk to your OPSEC. My point is that there are a lot of factors to consider, and so it would be foolish to say that you can be 100% anonymous and secure by following a few steps. However, as you have correctly stated, there are definitely things you can do to keep yourself relatively safe from the majority of people.

If this was directed at me, read my last post. I'm not saying that there's no point of being mindful about your OPSEC and following security practices - in fact I definitely believe that you should do these things, but it is extremely foolish, arrogant and ignorant to think that you can be 100% secure when pretty much everything the average person uses regarding technology is not made by them.

If the U.S. government really wants you, they'll catch you. Period.

However, like you said, there are things you can do to make their jobs a living hell.