

Forum:[Hack Forums](#)

Thread: [Do you bother with browser fingerprint in E-W?](#)

frostfox - April 28, 2019, 9:07 am

Like you go with it or you try to make your browser fingerprint more common? or change it regularly?

CapitalGainz97 - April 28, 2019, 9:35 am

(Apr 28, 2019 09:07 AM)frostfox Wrote: [\[CITE\]](#) Like you go with it or you try to make your browser fingerprint more common? or change it regularly?

Well if you don't wanna get caught you should but you need more than just Canvas Defender to beat machine tests being run on your screen etc. Try meddling with fresh and up to date headers of common browsers & machines (OSX, Windows, Linux, iOS and Android), some will brake some will work. Keep your notes and advance your techniques until you can immitate most of them. Spoofing the timezone and messing with it's own subheaders is cool too and you can also manipulate the window (not the whole box) size. Mozilla's responsive design mode can give you a glimpse of what I'm saying but essentially it's crappy itself. Names can't be named but some browsers provide the tools you need but you need to pay upwards 2 grant for them.

Delanata - April 28, 2019, 9:42 am

Use a virtual machine if that the case.

frostfox - April 28, 2019, 10:19 am

(Apr 28, 2019 09:35 AM)CapitalGainz97 Wrote: [\[CITE\]](#) Well if you don't wanna get caught you should but you need more than just Canvas Defender to beat machine tests being run on your screen etc. Try meddling with fresh and up to date headers of common browsers & machines (OSX, Windows, Linux, iOS and Android), some will brake some will work. Keep your notes and advance your techniques until you can immitate most of them. Spoofing the timezone and messing with it's own subheaders is cool too and you can also manipulate the window (not the whole box) size. Mozilla's responsive design mode can give you a glimpse of what I'm saying but essentially it's crappy itself. Names can't be named but some browsers provide the tools you need but you need to pay upwards 2 grant for them.

Can i have the names?

Johny498 - April 28, 2019, 5:19 pm

hm... i dont know what are you guys even talking about .. how can i learn more about this it seems like something i should be aware off?

THC - April 28, 2019, 5:29 pm

(Apr 28, 2019 05:19 PM)Johny498 Wrote: [\[CITE\]](#) hm... i dont know what are you guys even talking about .. how can i learn more about this it seems like something i should be aware off?

Browser fingerprinting is a technique used to generate a unique identifier for a person's browser. There's a variety of ways this can be done, the method people are discussing here is fingerprinting based on canvas noise. Every browser generates HTML stuff slightly differently, so if you generate an image on a client, then record the way that image was created, you can identify the same user if they visit the site again. Roughly.

Theres a lot of other things that can go into fingerprinting, such as browser audio elements, User agent settings, installed plugins, WebGL, font detection, etc. Plenty of information on it, give it a google.

I personally use this: <https://addons.mozilla.org/en-US/firefox/addon/canvasblocker/?src=ss>
To defend against HTML canvas fingerprinting. Open source, on github.