GOOGLE KNOWS EVERYTHING YOU HAVE CLICKED ON ONLINE!

Ninja Bits: The assistant professor at Princeton, Arvind Narayanan, who is a graduate student from Steven Englehardt has conducted a large massive study upon how exactly websites track their users by utilizing different techniques.

The results displayed on the Princeton Web Census research can show us that the massive search engine Google, through thousands upon millions of multiple domains, possess the ability to track users upon and 80-percent of all that tops the 1-million domains.

The serial tracker – Google!

The researchers that has revealed the Google-owned domains, in which browsers are able to load the tracking code, holds the accounts for the top 5 of the most popular trackers and still continues as the 12 of the top 20 tracker domains.

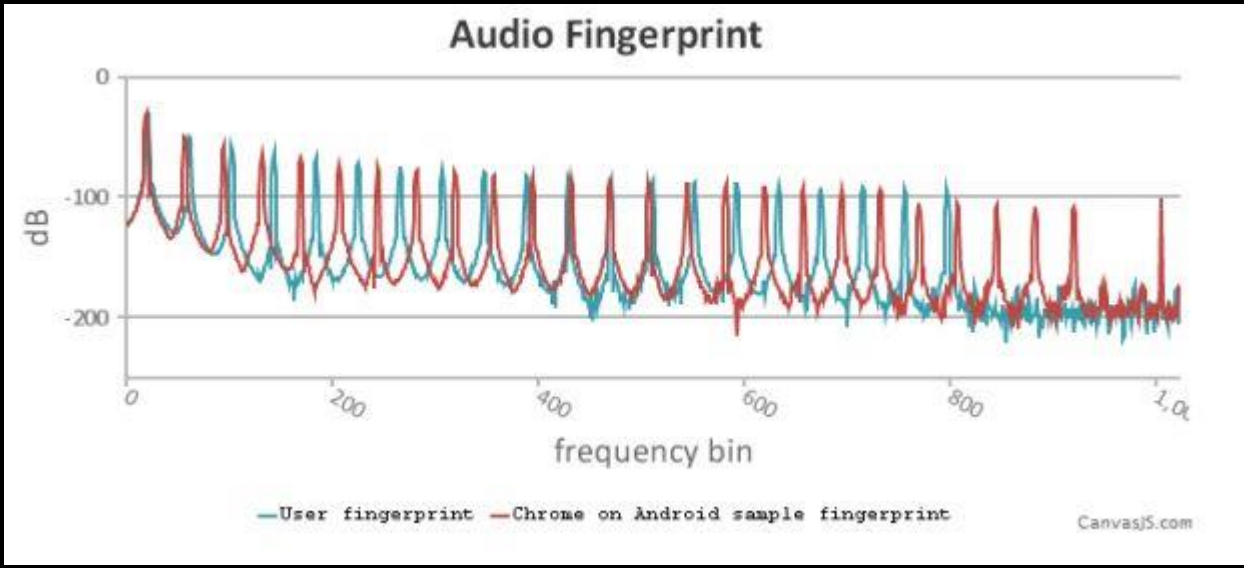
Fact: After performing the study of the top 1-million sites, the researchers has also discovered that there are just over 81,000 different domains in which has also enabled the tracking code loaded on their website. As we take a closer look into this data, those researchers have also proclaimed that there are only 123 of third-party trackers that are found just above one-percent of all websites.

This provides suggestions that the total number of the third party trackers in which are utilized regularly will also encounter on a normal daily bases is actually rather small. This effect is accentuated as we look into the different third-party entities in which are owned by the same entity. We also know that Facebook, Google, and even Twitter holds the only third-party entities that are clearly present on more than ten-percent of websites.

What does all of this mean? In essence, there is a greatly high chance that as you visit a website, or even click on a link, that one out of three major companies, if not all of them combined, will already know

about it. This holds most possible through Google, in which the company loads a type of tracking code upon four out of five websites.

The third party trackers are moving to implement an audio-based fingerprinting.



In order to fully collect their data, the researchers had to utilize a special piece of software that they had to customize. They called their software "OpenWPM", in which they have generously hosted online as open-source. The OpenWPM loads several websites instead of Chrome, Firefox, and even Internet Explorer. Thus collecting several packets of data upon the tracking technology that is loaded onto each page.

This OpenWPM will search for third-party Javascript files, Flash objects, cookies, fonts, and even fingerprinting techniques. Such as the ones that utilizes the HTML5 canvas, audio context, and API's as well as Negate local IP discovery.

However, out of all of the third-party entities, the newest one of the tracking technology family that the researchers have discovered is that also happens to leverage the audio-context API. Normally other third-party tracking entities use will use it in order to send a low-frequency sound to a user's computer, this will measure how the user's computer process the data. Thus resulting in creating a unique fingerprint that is solely based upon the user's hardware and other software capabilities.
If you would like to be able to check your own audio fingerprint, there is a "demo-page" that is setup by the researchers for you to use.

The user tracking entities are everywhere.

As the results from the Princeton survey are not much of a large surprise to several of us, as we have seen something quite similar carried out by researchers from MIT and Oxford. Their researcher was published earlier this week that had also reveals that the Twitter location tags, that on just a few tweets, you can see a lot of the details about a specific accounts owner. Such as their real-world address, their hobbies, and even medical history. However, this data was collected by Twitter and is using it to deliver more advertising to specific targets.

However, tracking entities are not entitled to just the world wide web. Other recent studies, such as the one by the researchers from Stanford, has shown that phone call as well as phone's metadata can be utilized in order to infer with your phone details, which provides personal information about you. While your cell phone carrier is not listening to your phone calls, they may know just as much about you as Google, if not even more so.

All of the studies performed has also revealed that it is clearly becoming much harder to maintain a low profile while carrying out your personal life online or even on your phone. Some known users will block the HTML5 canvas fingerprinting, however, they may also use their cell phones on a more regular basis. For those who do not use the mobile phones, then the WGATC will reveal their real IP address, even if they are hiding behind a wall of VPN's. However, regardless of how

different users may attempt to avoid the third-party trackers, there will always be someone in shadows watching us.

Sources: News. Softpedia { } GitHub { } Princeton Web Census { } OpenWPM { } News. MIT { } PNAS { }