If you are an activist. Part two: “The provider is watching you”

By admin fortanga.org5 min
February 7, 2020
View Original

In the previous article we talked about what SORM is and what information about you can be obtained from this system.

In this article we will tell you what SORM-2 is and how to protect yourself from tracking on the Internet.

If SORM (System of Operational Investigative Activities) is “wiretapping” of telephone and SMS, then SORM-2 is a system for listening to mobile communications via the Internet and monitoring the content of Internet connections of the data network, in other words, monitoring the Internet.

Let's start with the fact that SORM-2 is a server running on the provider's equipment, connected to the FSB console. Intelligence services have constant access to databases without operators, through a special communication channel. Information according to the SORM-2 standard is stored according to various data from a day to three years. But with the entry into force of the Yarovaya Law,

SORM-2 will give way to SORM-3 , which will work in a similar way, but is designed for long-term storage of traffic information.

That is, it will be possible to listen to you not from the moment when the operatives made a decision about this, but to receive information about your conversations that took place much earlier.

SORM-3 the newest version, ensures the unification of all the above systems and additionally controls part of the VPN servers, listens live on Skype, ICQ, satellite communications and a number of other innovations. But the key factor of SORM 3 is a single global database that is interconnected with various areas of SORM.

SORM is available in all data centers of the country, at all providers of different levels, at traffic communication points, on all the largest search engines, on all the largest social projects (a la Odnoklassniki, VK).
Moreover SORM (not a system, of course, employees) very actively interact with programmers who write communication systems (IP telephony, instant messengers, etc.) . etc.) or, roughly speaking, they facilitate the introduction of bookmarks

(backdoors) into these programs in order to be able to eavesdrop.

How can you protect yourself from tracking?

Let's first consider a simple situation: You type in the address bar, for example, fortanga.online From a technical point of view, this address looks different, like this: https://fortanga.org This is an unencrypted data transfer protocol. Hence the first conclusion: the provider sees the full addresses of unencrypted domains, that is, it knows where exactly you “sit” on the Internet.

If you wish, you can easily find out your password for the site and read every word of your unencrypted correspondence on social networks, every comma that you send to your friend. Also, downloading via torrent occurs without encryption - communication between the tracker and the torrent client takes place via HTTP. For the provider, everything is transparent: specific torrents (movies, games) and all the statistics on them are visible (when the download started and completed, when and how much you “distributed”).

If you access a site with encryption, for example, https://fortanga.online (HTTPS, and not HTTP) (or to any online chat or online store), then the provider

knows only the IP address of the server, the connection time to it, the amount of traffic to it and nothing more . All other data is transferred from your device (computer, smartphone) in encrypted form.

You should also remember that the provider does not store all your traffic, but mirrors it into SORM servers (technical means of operational-search activities), which are controlled by the FSB and the Ministry of Internal Affairs. Due to the huge volume of traffic passing through the Internet provider, it can be assumed (since there is no reliable information about SORM in the public domain) that the storage period of data on these servers is not so long, but according to SORM -3 there is no specific information yet.

The telecom operator only processes your traffic, classifies it and keeps logs about it. For example, the provider knows that on June 26 at 10:10 a user with the login The Pink Eagle turned on the computer, went online, connected to the fortanga.online node, transferred 2 GB of traffic to it, and disconnected at 11:00. The content entropy was 99% (this term means that the data was transmitted in encrypted form). The operator is obliged to store these logs for 3 years and provide them to the FSB authorities by accessing their databases.

How to hide sites and traffic from your ISP?

Let's consider a more complex case: You are using VPN. In this option, the provider sees encrypted traffic sent to a specific IP. You can find out a lot from the IP address, including calculating the entire range of addresses allocated for virtual servers. It is impossible to track the further direction of the transmitted data on the provider’s equipment unless you conduct targeted surveillance of the subscriber, comparing user traffic with server traffic. However, even surveillance is not always required, since the operating system can suddenly “set you up.” When the VPN is randomly disconnected, Internet traffic begins to flow “directly” in the clear, and then the provider immediately sees your real IP.

Everything that has been said about virtual networks applies in full to the increasingly popular browser extensions. They may use completely different technologies, but it is possible that many of them are made to track anonymous users.

Finally, let's look at the most difficult option: You use TOR. In this case, the provider will not see the address of the site you are visiting. It will only receive the IP address from which the data streams are coming, and this address will change to a new one

automatically. Today there is no technology for decrypting TOR traffic, but systems for its accurate detection already exist. The use of TOR in itself is considered a suspicious action, and this fact, recorded in the provider's logs, may become the basis for more careful monitoring of the user.

In conclusion, I want to reduce the degree of paranoia: the provider can monitor you, but it is unlikely that he will do this of his own free will. Yes, operators cooperate with "authorities", yes, operators record logs, but until the moment you actually commit illegal actions on the Internet, no one will watch you. As a rule, no one needs this, plus it requires a lot of money. From the logs, only what is commercially profitable for operators is quickly calculated: for example, data that you often visit the website of another provider.

Try this, and perhaps the very next day your telecom operator will call and ask if you are satisfied with their service.

In any case, remember that there is no absolute anonymity on the Internet. Absoluteness, in general, in practice often becomes relativity :)

Based on Internet materials