Western Intelligence Agencies Stole 97 Billion Global Internet Data in Just 30 Days

Description

Western intelligence agencies are once again acting illegally, stealing data around the world and violating the sovereignty of the countries.

In a recent report revealed by the Chinese media, details of the data capture power of the so-called " ***Five Eyes",*** *the data sharing network of the secret services of the five Anglophone powers, were shown. In just a month, billions of data were stolen, and phone calls violated, creating a scenario of insecurity of privacy around the planet.*

The report comes from a cybersecurity agency called Anzer, which gave information to the Chinese newspaper Global Times last Monday, June 13th.

In all, 97 billion global internet data were stolen, in addition to 124 billion phone records infringed in the last thirty days alone. The main agencies reported by Anzer are US intelligence organizations, but there is also involvement of **all agents participating in the scope of the "Five Eyes", which brings together the secret services of the US, Canada, UK, Australia and New Zealand.**

According to Anzer's agents, such clandestine operations – called "black hand operations" – are mostly carried out by **Tailored Access Operations (TAO), which is the cyber warfare agency that directly serves the US National Security Agency (NSA).**

The report says that recently increasingly powerful cyber weapons have been used in data theft operations, being capable of indiscriminately capturing information from billions of internet users around the world simultaneously.

An anonymous expert quoted by Global Times commented on the topic saying:

"The NSA's global indiscriminate intrusion has long been supported by a vast and sophisticated network of weapons platforms, of which TAO is an important weapon maker. Some of these weapons are dedicated to the products of US internet giants such as Apple, Cisco and Dell, and have been developed with the support and full participation of these internet giants (…) The US is taking highly

engineered cyber weapons as the winning advantage in future cyber warfare, and is investing resources and increasing chips regardless of cost, bringing endless hidden dangers to global cyber security".

One of the main advanced cyber espionage instruments used by the NSA/TAO to maintain this type of **massive data theft strategy is the so-called NOPEN**. Such a weapon had already been denounced by the Global Times, in May, and consists of a mechanism capable of accessing various types of confidential information on any equipment using the Unix/Linux system. Indeed, the weapon is used not only to steal secret files, but also to redirect network communication and view information on other computers connected to the assaulted one.

Now, however, it is revealed in the Anzer's report the existence of another platform used by the NSA to carry out such operations, dubbed the "boundless informant". Such a weapon, hitherto unknown, would have an even greater ability to collect, manage and analyze massive data, expanding TAO's ability to steal information, which explains the power to acquire so much data in such a short period of time (97 billion in 30 days).

In fact, these reports point out that clandestine cyber activities have been systematically practiced by official agencies of the governments of some of the main world powers, mainly the US.

It is a delicate and controversial finding. In general, there is a consensus among experts that cyber weapons should only be used for specific and circumscribed operations, **considering that their potential for privacy violations can unnecessarily affect the security of individuals.** When it is revealed that US and every Five Eyes country systematically promotes this sort of infringement, it sets a precedent for other nations to respond with the same attitude, culminating in worldwide data insecurity.

To avoid this, it is necessary to neutralize the threats already identified, creating mechanisms to prevent the Five Eyes' agencies from continuing to steal information.

A joint reaction on the part of international society is urgently needed. It is not acceptable that cyber weapons are used indiscriminately and put data security at risk. In a progressively technologically integrated world, all individuals are threatened by these clandestine activities, which makes the current situation really unsustainable.

The practice of "black hand operation" must be eradicated from the cyber battlefield. Perhaps the only way to do this is through a new international treaty of global dimension, which counts on the goodwill of all the world potentials to sign a document renouncing the use of weapons that promote indiscriminate data theft.

by Lucas Leiroz

Featured image is from InfoBrics

Category

1. Crime-Justice-Terrorism-Corruption

2. Main
3. Politics-Geopolitics-Gov.-Events
4. Science-Tech-AI-Medical & Gen. Research

Date Created
06/20/2022