<u>Digital celebration with bitter taste</u>

By Lautaro Rubbi, research professor at the
Institute of Social Sciences of UADE Foundation - CONICET

On last month we celebrated the worldwide Information Society Day and the Internet Day. The reasons to celebrate were many. According to the latest report of the International Telecommunication Union, 47% of the world's population already uses the internet, and not just on computers. New technologies allow connection and remote management of cameras, traffic lights, crop sensors, public lighting and even high security databases. More and more every day, everything around us depends on the internet to work. The possibilities seem endless. However, there are as many reasons to celebrate as to reflect and be cautious.

In first place, the promises of a more egalitarian world society thanks to the new technologies remain unfulfilled. The distribution of connections is as inequitable as that of wealth, concentrating on states and populations with high purchasing power. Iceland is in first place, with 98.2% connectivity, followed by other Nordic countries, Central Europe and some Asians. But it is also highly limited in other countries. Chad barely reaches 2.7%.

But inequality is not what worries the most on these days. The fragile security of the networks is today the main discussion topic. The possibility of penetrating the systems of virtually any device is a reality and the theft of business information is an ever-present danger. According to Cisco's 2017 annual report on cybersecurity, more than one-third of the organizations that suffered attacks in 2016 reported substantial and million-dollar losses in consumers, business opportunities, and equity value.

The theft of personal financial information and intrusion into devices and social networks of public figures is also common. In the weeks leading up to the elections in France, intimate documents of the finally elected Emmanuel Macron were supposedly extracted by computer attacks from Russia and released. The event made little effect on the image of the then candidate. But that depended largely on the caution with which the media and the civil society treated the information. Similar events occurred during the presidential campaign in the United States with a much greater media, political and social impact.

Cyber Intrusions don´t affect just politicians. In may, a massive Ransomware-type attack left more than 50,000 machines infected in more than 150 countries. Blocking the user's files until he makes a rescue payment using Bitcoins, this type of attack is rather common and even easy for experts to release. It represents 72.75% of malicious attacks, according to the latest reports from Kaspersky Lab and PandaLab. However, the international reach of the virus was practically unparalleled in history, leaving out of service entire hospitals in the United Kingdom, multinational corporations of the size of Fedex, Renault and Telefónica and even universities in Russia and the United States. The attack could be avoided by simply updating the latest security patches Microsoft had released in March of this year.

In an attack of similar characteristics, computer systems in Europe, Asia, and the United States were hit on the last days by a ransomware attack that has crippled tens of thousands of computers worldwide. Ukraine seemed to be the main target of the hack, which reached computers belonging to the Ukrainian government and the postal service, as well as banks, an international airport, one of the largest communications companies, the national railway company and the Chernobyl nuclear facility. A number of other European companies, including Rosneft, the Russian energy giant; Saint-Gobain, the French construction materials company; and WPP, the British advertising agency, also said they had been targeted.

But surprisingly, this ransomware was for sale on the Dark Web for months, available as "a service". That means anyone could use it, encrypt someone's systems and demand a payment to unlock it; if the victim pays, the authors of the ransomware get a cut of the payment. That distribution method makes the attribution of responsibility much difficult. And for worst, this software does not have a "kill switch" to turn it off as the ransomware of the previous attack had, making it even more dangerous. So it is yet unclear who was behind this cyberattack and the extent of its impact. Cybersecurity researchers have also questioned whether collecting ransom was the true objective of the attack or if it is related to more political and geopolitical purposes.

These have not been the first such attacks and will certainly not be the last. The cybercrime sections of the various national and provincial police forces already accustomed to follow this type of cases, which require little technical knowledge. Pre-programmed Ransomware packages are usually sold on the Dark Web for immediate use, though they usually include other hidden viruses that paradoxically end up attacking the buyer.

In the world of the Internet, complexity is necessarily associated with vulnerability. The architecture of the World Wide Web was never been thought of in terms of security and multiple studies have shown that the need and concern for protection often arrives later than the creation of the new technologies. We must accept it, although its effects may be different, digital crimes are as common today as armed robberies. Cybersecurity should already be part of our daily lives.

The Internet offers us a future of new possibilities. But the challenges we face are also new. Today, nobody is exempt from the theft of information and the dangers that circulate on the network. Clear awareness of this is an essential step towards adopting best practices to protect ourselves. The vast majority are rather basic and do not require any specialized knowledge.

It is true that becoming a target of a persistent and systematic attack by a hacker is likely to imply that even the best defenses will be violated. This is well known by governments and large corporations. But it is also true that most of the common public is not an attractive target for such attacks, so costly in time and resources. To avoid most attacks aimed at massive targets, it would be sufficient simply to update the antivirus and the corresponding security patches, use different passwords for different portals and avoid opening files of unknown content or origin. These basic measures will be enough to keep us safe most of the time. As long as solid and clear technical measures are not taken, individual caution is the best policy. If the whole world becomes aware of this, that will be reason enough to cheerfully commemorate another year of the internet miracle.

Artículo Publicado en:

https://www.estadointernacional.com/digital-celebration-with-bitter-taste/