Russian cyberattacks

30.12.2022

With the ongoing war in Ukraine, in the Polish cyberspace, there are more and more occurrences classified as computer incidents, including attacks perpetrated by Russian hackers. This is a response of the Russian Federation to the Poland's support provided to Ukraine and an attempt to destabilise the situation in our country.

Since the beginning of the Russian invasion against Ukraine Poland has been a constant target of the Kremlin's hybrid actions, including attacks in cyberspace. Recently this hostile activity has intensified. This is the

consequence of our commitment to help Ukraine but also of the fact that Poland is strongly advocating in the international arena for providing help to Kyiv. Through hostile operations in cyberspace Russia wants to exert pressure on Poland, as a frontline country and a key Ukraine's ally on the NATO eastern flank.

Both public administration domains and private companies, the media and ordinary users become the target of hacker attacks. Entities from strategic sectors, such as energy or armaments, are particularly at risk. Some of these hostile campaigns can be linked directly to the activities of pro-Russian hacking groups.

This was the case, for example, with the recent attack on the website of the Polish parliament (Sejm). The CSIRT GOV team operating in the Internal Security Agency (ABW) identified problems with the accessibility of the sejm.gov.pl website. Data analysis showed that the website's unavailability was the result of an attack carried out by the pro-Russian group NoName057(16). This group on the Telegram portal has set the parliamentary website as one of its goals. This attack was a response to the adoption by the Sejm of the Republic of Poland of a resolution recognizing Russia as a state sponsor of terrorism.

Such incidents in cyberspace are retaliatory actions typical of Russia, which are a response to steps taken by other countries, that are unfavorable and inconvenient for the Russian Federation. Hacker groups linked to the Kremlin use ransomware, dDos and phishing attacks, and the goal of hostile actions coincides with the goals of a hybrid attack: destabilization, intimidation and sowing chaos.

False structures are also used for aggressive actions, such as websites impersonating real websites. In the first days of December, the CSIRT GOV Team received information about the registration of a phishing website impersonating the website in the government domain gov.pl. The content of the fake website suggested that the President of the Republic of Poland signed a decree on compensation for Polish residents, financed from European funds. The "I'd like to know" link led through a phishing process and then redirected to a phishing payment card page under the guise of charging a verification fee to pay compensation. Thanks to the intervention of the Internal Security Agency, the website was blocked. This is a typical operation aimed at sowing chaos, undermining the state, but also collecting personal data and extorting money.

Every attack in cyberspace pursues complex objectives and has various implications – social, political or financial ones. More and more often cyberattacks are used in order to spread Russian disinformation and serve Russian special services to gather data and vulnerable information. The operation that is carried out using simultaneously both of these methods is the „GhostWriter" campaign. It consists in attacking email addresses and accounts in social media of public figures in the CEE countries, mainly in Poland. The authors of this campaign are trying to seize information resources for the purposes of the Russian disinformation. In recent months this operation has been focused on actions against Poland.

Taking into consideration an increasing scale of threats, the Polish cyberspace is constantly monitored as far as potential dangerous incidents are concerned in order to react to them as fast as possible. At the same time, it is important to implement measures in order to prevent attacks. In Poland, the Prime Minister has also introduced the third security alert CHARLIE-CRP which is related to the cybersecurity and responds to growing threats in cyberspace.

Government Plenipotentiary for the Security of Information Space of the Republic of Poland.