The NCCC at the NSDC of Ukraine warns of a new mechanism of attacks on Ukrainian infrastructure

rnbo.gov.ua/en/Diialnist/4820.html

Ваш браузер є застарілим і не підтримує сучасні веб-стандарти, а так само становить потенційну загрозу вашої безпеки.
Будь ласка, встановіть сучасний браузер

Starting from February 18, this year, the National Coordination Center for Cybersecurity at the NSDC of Ukraine records massive DDoS attacks on the Ukrainian segment of the Internet, mainly on the websites of the security and defense sector.

In particular, attacks were carried out on the websites of the Security Service of Ukraine, the National Security and Defense Council of Ukraine, resources of other state institutions and strategic enterprises. It was revealed that addresses belonging to certain Russian traffic networks were the source of these coordinated attacks.

During the response and analysis, it was found that the attackers used a new mechanism of cyberattacks, which had not been observed before in similar incidents.

In such a way, during an attack, vulnerable government web servers are infected with a virus that covertly makes them part of a botnet used for DDoS attacks on other resources. At the same time, security systems of Internet providers identify compromised web servers as a source of attacks and begin to block their work by automatically blacklisting them. Thus, even after the end of the DDoS phase, the attacked websites remain inaccessible to users.

The NCCC experts are ready to provide consultations and technical assistance to detect and respond to this type of cyberattack. In case of detecting the compromised websites, DDoS-attacks, please notify the National Coordination Center for Cybersecurity (report@ncscc.gov.ua) immediately.

Print Version

Organization of the National Security and Defense Council of Ukraine