Мусулега Є., курсант ВСФП
Національна академія внутрішніх справ
Консультант з мови: **Гончаренко Н.І.**

LATEST CYBER ATTACKS. WHO'S IN CHARGE?

The cyberattack of 27 June 2017 isn't the first time Ukraine has been under cyberattack. In December 2015, power company Prykarpattyaoblenergo suffered a major attack that led to blackouts across western Ukraine.

About 230,000 Ukrainians were plunged into darkness for six hours after hackers inserted malware into control systems of part of the oblast grid.

Ukraine blamed Russia for the attack, and the malware used, BlackEnergy, has its origins in Russia, according to experts. However, there is no definitive link between the cyberattack and the Russian government, according to U.S. officials.

The malware was reportedly delivered via spear phishing emails with malicious Microsoft Office attachments.

A year after that, another attack hit an electricity transmission facility outside Kyiv. In a report by tech magazine Wired, cybersecurity firms that have since analyzed the attack said it was executed by a "highly sophisticated, adaptable piece of malware" now known as "CrashOverride", a program coded to be "an automated, grid-killing weapon".

And while nobody really knows how to deal with the computer virus, companies in Ukraine and across the world are still grappling with the effects of a major new ransomware cyberattack that struck their computer systems.

The client services of Kyivenergo, which provides Ukraine's capital with electricity and heat energy, were still limited on June 29 due to the virus attack.

On June 29, Ukraine's SBU security service issued a statement that it, together with the U.S., FBI, the UK's NCA, Europol and other leading cyber security companies and specialists, are currently investigating the spread of the NotPetya virus, trying to identify those behind the attack.

At the same time, Ukrainian authorities together with global tech company Cisco are working on software to recover blocked computers.

Cisco spokesperson Yulia Shvedova told that such attacks are common, and that they will continue to happen as hackers develop more and more sophisticated techniques.

Neil Walsh, head of the UN Global Program on Cybercrime, called the current virus more sophisticated than the WannaCry ransomware virus, which wreaked havoc worldwide less than two months ago. Reportedly the work of North Korean hackers, WannaCry affected computers that had failed to install one of the latest updates to Windows.

Among the major victims of that ransomware were the British National Health System, the Russian Ministry of Internal Affairs, and Japanese carmaker Nissan.

Walsh said it still was unclear whether Ukraine was the main target of the NotPetya virus. Cyber security experts were also working to identify the attackers, he said.

"This could be anything from a kid sitting in his basement… to a nation state", he said.

Список використаних джерел

1. www.pravda.com.ua
2. www.bbc.com
3. www.kyivpost.com