Daily Sabah.- 25.01.2019

Ukraine says it sees surge in hackers targeting upcoming elections

Україна заявила, про активність хакерів, орієнтованих на на майбутні вибори

Начальник Української кіберполіції Сергій Демедюк повідомив, що хакери, які, ймовірно, знаходяться під контролем Росії, активізують зусилля для того, щоб зірвати президентські вибори в Україні, пише турецьке видання. Зловмисники використовували вірусно-інфіковані вітальні листівки, торгові запрошення, пропозиції для оновлення програмного забезпечення та інші шкідливі "фішингові" матеріали, призначені для крадіжки паролів і особистої інформації. За десять тижнів до виборів хакери купували особисті дані чиновників, сказав Демедюк, сплачуючи в криптовалюті на темній павутині. За даними кіберполіції, ще не зафіксовано проникнення до виборчої системи, але вони очікують ще більших нападів за місяць до виборів, коли регіональні представництва комісії почнуть працювати

https://www.dailysabah.com/europe/2019/01/25/ukraine-says-it-sees-surge-in-hackers-targeting-upcoming-elections

REUTERS

Ukrainian Cyber Police Chief Serhiy Demedyuk speaks during an interview with Reuters in Kiev, Ukraine November 2, 2017. Picture taken November 2, 2017. (Reuters Photo)

Hackers likely controlled by Russia are stepping up efforts to disrupt Ukraine's presidential election in March with cyberattacks on electoral servers and personal computers of election staff, the head of Ukraine's cyber police said on Friday.

Serhiy Demedyuk told Reuters the attackers were using virus-infected greeting cards, shopping invitations, offers for software updates and other malicious "phishing" material intended to steal passwords and personal information.

Ten weeks before the elections, hackers were also buying personal details of election officials, Demedyuk said, paying in cryptocurrency on the dark web, part of the internet accessible only through certain software and typically used anonymously.

"There are constant attacks - they go from simple (software) to applications that one or another employee uses," he said, adding they were reminiscent of cyberattacks on the country's energy, transport and banking systems seen since 2014.

"Payment occurs in cryptocurrency in most cases ... and from the same wallets that were used to finance the previous attacks. This indicates that the same hacker organizations that are under the control of Russian special agencies are engaged in this," Demedyuk said.

In Moscow, the Kremlin did not immediately respond to a request for comment on Demedyuk's remarks.

Relations between Ukraine and Russia plunged following Russia's annexation of Crimea in 2014, and Kiev has accused Russia of orchestrating large-scale cyberattacks as part of a "hybrid war" against Ukraine, which Moscow repeatedly denies.

In one of the attacks the "NotPetya" malware in 2017 hit thousands of computers not only in Ukraine but also around the world, disrupting shipping and businesses.

Ukraine imposed martial law in November, citing the threat of a full-scale invasion after Russia captured three of its vessels in the Kerch Strait.

Pro-Western President Petro Poroshenko, likely to stand in the elections, said this month that the Kremlin had developed a huge arsenal of methods for interference in the elections.

"This is not just our take. The Russian meddling to influence Ukraine's elections is well under way," Petro Poroshenko told foreign diplomats.

His main opponent in the polls is opposition leader and former prime minister Yulia Tymoshenko, also pro-Western and with a following among Ukrainian nationalists.

According to the cyber police, no infiltration into the electoral system has been recorded yet, but they expect even larger attacks a month before the elections when the commission's regional offices will start working.

The hackers buying personal details of election officials were concentrating on civil servants and employees who keep the commission's equipment running, he said.

On phishing attacks, Demedyuk said "virus-laden New Year's greetings on behalf of government bodies or the governments have become so widespread that they are just overwhelming."

"Such mailing lists, spam letters are sent to them and their relatives, which contains malware to control their computer equipment. This is the easiest way, but it is effective."

The cyber police worry that critical infrastructure in sectors such as energy and banking may again become the object of cyberattacks during or before the elections using malware to create so-called 'back doors' for a large coordinated attack.