Стеценко О., курсант
Національної академії внутрішніх справ
Консультант з мови: **Гончаренко Н.І.**

POWERFUL CYBERATTACKS IN UKRAINE. JUNE 2017

Some of the biggest state-owned and private companies in Ukraine stopped functioning on the afternoon of June 27 due to what appears to be the biggest -ever ransomware attack in the country's history.

A new outbreak of ransomware known as Petya that has been active since spring 2016 hit computers across the globe, but Ukraine was apparently hit the hardest.

The virus blocked the computer networks of Ukraine's critical infrastructure, telecom companies, banks, postal services, big retailers, and government bodies.

The ransomware took over the computers, encrypted data and demanded a ransom of $300 in bitcoins, a digital currency used to carry out untraceable transactions.

Firms around the globe are now reporting that they have been hit by a major cyberattack, including British advertising agency WPP, Dutch transportation company APM, several oil and gas companies in Russia, as well as companies in Spain and France.

In Ukraine, the attack has affected state-owned Oschadbank, private Ukrgazbank, energy companies Kyivenergo and Ukrenergo, national telecommunications operator Ukrtelecom, mobile carrier Lifecell, postal companies Ukrposhta and Nova Poshta, Kyiv Boryspil International Airport, DIY chain Epicenter, petrol retailers, and several media companies, including Channel 24 and Korrespondent news website.

Most of the affected companies had to stop or limit their services due to the attack.

The computers of the Cabinet of Ministers of Ukraine were infected with the virus, too, according to Deputy Prime Minister Pavlo Rozenko, who published a screenshot of one of the computers with a black screen and hackers' warning.

Oleksander Pertsovskyi, first deputy CEO of national postal service Ukrposhta, says most of the company's offices now have to do without computers.

"We've suffered. As well as many other Ukrainian companies," Pertsovskyi told the Kyiv Post. "The virus spread so fast that we decided to switch off all the computers and servers."

Ukrposhta plans to have its computers back in work by June 29.

The Petya ransomware attacks only those computers that use Microsoft Windows. Microsoft Ukraine would not comment on the situation now, saying only that the newest Windows updates can help protect the systems.

If one computer in a local network is infected with the virus, it quickly spreads among all the computers in the network. The virus encrypts the files and demands a ransom of $300 to get their data back. So far the bitcoin wallet used in the attacks in Ukraine has received 13 transactions.

The Security Service of Ukraine (SBU) stated that the attack was a planned operation.

"(It) was planned in advance and happened in several stages," the statement reads.

Now SBU, the State Service of Social Communications, the cyber police, and representatives of some of the antivirus laboratories study the samples of malicious software and work out ways to neutralize it. In the near future, SBU plans to develop and send recommendations for protection against the cyber attacks.

Volodymyr Flyonts, an IT developer and one of the creators of Prozorro electronic procurement system, said many state companies became vulnerable to the virus because they failed to timely update their systems.

"Our government offices have lots of Windows XP and nobody cares there about updating them. That's why they so easily became targets of the virus," he told the Kyiv Post.

Viktoria Syumar, a lawmaker for People's Front, links the cyber attack with the Russian hackers:

"Russian secret services show and peculiar humor with the virus Petya," she wrote on Facebook, referring to Petya being short for Petro, the first name of Ukraine's President Petro Poroshenko. "But they very seriously show a necessity to pay an attention to the cyber safety no less than to real war danger."

Список використаних джерел

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