сфери суспільного життя, у тому числі й інформаційну [8, с. 49]. При цьому, кіберпростір є своєрідним «провідником» інформаційних процесів і домінуючою частиною інформаційної сфери сучасного соціуму.

Аналіз зарубіжного досвіду правової інституалізації кіберпростору свідчить про те, що характерною рисою цього процесу є прив'язка до проблем інформаційної безпеки. Так, в доповіді Міністерства оборони США "Операції в кіберпросторі", кіберпростір визначається як глобальний домен в інформаційному середовищі, що складається з взаємозалежної мережі інформаційних технологій, інфраструктури та резидентних даних, включаючи Інтернет, телекомунікаційні мережі, комп'ютерні системи та вбудовані процесори та контролери. Аналогічна дефініція кіберпростору застосовується в об'єднаній оборонній доктрині Міністерства оборони Великобританії [9, с. 5].

В Україні кіберпростір також розглядається, перш за все, з точки зору інформаційної безпеки держави. Так, в Стратегії кібербезпеки зазначається, що кіберпростір поступово перетворюється на окрему, поряд із традиційними "Земля", "Повітря", "Море" та "Космос", сферу ведення бойових дій, у якій все більш активно діють відповідні підрозділи збройних сил провідних держав світу [10].

Слід відзначити, що універсальність та глобальність кіберпростору обумовлює необхідність встановлення міжнародних стандартів щодо його захисту. При цьому, перед міжнародним співтовариством виникають проблеми, які виникала при впорядкуванні використання та захисту морського та космічного простору, а також Антарктиди [11].

Важливе значення для України має прийняття Закону «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки. Він містить легітимне визначення кіберпростору як середовища (віртуального простору), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утвореного в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечує електронні комунікації з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [12]. Аналіз цієї дефініції свідчить, що в її основу покладено функціональну сутність кіберпростору. Водночас, кіберпростір є більш багатогранним явищем і містить в собі технічні, енергетичні, інтелектуальні, контентні складові, сутність а зміст яких може бути предметом подальших досліджень з метою вдосконалення нормативно – правової бази в цій сфері.

Література:

1. Biocca F., Levy M. Virtual reality as a communication system / F. Biocca, M Levy // Communication in the Age of Virtual reality. – Hillsdale. – Lawrence Erlbaum Associates. – 1995. – 395 p. – p. 15 - 31.
2. Katsh E. Law in a Digital World: Computer Networks and Cyberspace / E. Katsh // Villanova Law Review. – 1993. – Vol. – 38. – Iss 2. – p. 403 – 486.
3. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д.В. Дубов. – К. : НІСД, 2014. – 328 с.

The ransomware “Petya” as a challenge to the cybersecurity of Ukraine, main factors of spreading this virus in the focus of Ukraine, the steps taken by the authorities to combat this phenomenon and suggest ways to improve such activities using experience of other countries

Victor Zhoghov
Deputy Chief of information systems administration
Department of information and analytical support
The main Department of the National police in Vinnytsia region
Senior lieutenant of police

Formulation of the problem

On June 27, a large-scale cyber attack was recorded in Ukraine using a new modification of the Petya ransomware, which partially affected companies in Russia, the United States, India, and Australia. A preliminary investigation showed that the pro-state Black Energy group that had previously attacked energy and financial organizations in Ukraine was behind the attack.

According to preliminary estimates, about 80 companies have been attacked, with the majority of them located in Ukraine. The list of victims includes large Ukrainian banks and enterprises, namely, Oschadbank, Ukrgasbank, Pivdenny Bank, OTP Bank, TASKombank, The Epicenter chain store, Kovalska industrial and construction group. Three major Ukrainian telecom operators, Kyivstar, LifeCell, Ukrtelecom, have also been affected.

State enterprises Ukrtelecom, Ukrzaliznytsia, Ukrposhta, Kievvodokanal, and state-run aircraft manufacturer Antonov informed they had come under a large-scale attack. The Boryspil international airport, Kiev subway, computer networks of the Cabinet of Ministers and the website of the Ukrainian government have also been infected.

Analysis of recent research and publications on this topic

Among those who investigated this problem were Constantin Lucian, Fabian A., Lee David, Burgess Matt, Jack Stubbs, Pavel Polityuk, Jack Stubbs, Matthias Williams, Volodymyr Verbyany, Stepan Kravchenko, Nicolas Weaver etc.

This article is intended to analyze the main factors of spreading this virus in Ukraine, the steps taken by the authorities to combat this phenomenon and suggest ways to improve such activities using experience of other countries.

Presentation of the main material

First of all ,the term “Petya” is explained as a type of malware and its basic capabilities.

Petya is a set of malware that affects computers running the Microsoft Windows operating system family. The program encrypts files on the victim machine's hard drive, as well as overwrites and encrypts the master boot record (MBR) - the data needed to boot the operating system. As a result, all files stored on the computer become inaccessible. Then the program requires a ransom in bitcoins for decoding and restoring access to files.

So, how did it appear in Ukraine?

According to law enforcement agencies, intruders committed unauthorized interference with the work of one of the personal computers of the software company Intellectual-Service, LLC.

Once they have access to the source code, they have installed a backdoor in one of the program updates, which installed “M.E.Doc” users on unauthorized remote access computers. This software update probably took place on 15.05.2017.

“M.E.Doc” program is one of the most well-known services for optimization of accounting operations in Ukraine. This software is used by virtually every other company in our country.

At the same time, it was found that the detected backdoor on the functional has the ability to collect the codes of the USREOU of the affected companies and send them to the remote server, download files, collect information about the operating system and user identification.

Also it is known, that after the backdoor has been triggered, attackers compromised user accounts to gain full access to the network. Then they got access to the network equipment in order to eliminate it. Using IP KVM, they downloaded their own operating system based on TINY Linux.

Intruders in order to conceal successful cyber-robots against the massive damage of computers and unauthorized collection of information from them in the same way, through the latest updates to the software “M.E.Doc” distributed the modified ransomware Petya.

The removal and encryption of operating system files was done to remove traces of previous criminal activity (backdoor) and to divert attention by simulating the extortion of cash from victims.

In addition, the virus spreads through spam messages that contain links to download files from Dropbox called “application folder-gepackt.exe”. When the file is downloaded and opened, the virus is activated.

Microsoft announced that 12,5 thousand computers were infected in Ukraine.

The authorities, in the person authorized to this body, namely: the Security Service of Ukraine, Department of Cyberpolice of the National Police of Ukraine, State Special Communications Service of Ukraine, State Center for Cyber Defense and Counteraction, National Cybersecurity Coordination Center began to investigate a serious computer attack that caused chaos on computer servers of the nation companies and institutions.

First of all, a source of malware was identified.

Also, the cyber police together with leading cyber security experts have been working to create a decryptor for decrypting files encrypted with malware.

Through social networks, the authorities conducted constant work with the population to provide advice on preventive measures to prevent infection, provided links to patches of security updates, etc.

The staff of the cyberpolice created a headquarters that provided real-time counseling round-the-clock on how to avoid infection with the virus.

Some institutions, such as Nation Bank of Ukraine announced the creation of the Banking Market Cybersecurity Center (CSIRT-NBU) for the prompt response and exchange of information between all actors of the banking market and law enforcement agencies in real time.

All these measures enabled special agents of the cyberpolice department, together with the Security Service of Ukraine and prosecutors, to stop the second stage of the cyberattack Petya. Cyberpolice blocked the mailing and activation of the virus from the servers of the informational system "M.E.Doc". The attack was stopped. The servers with the traces of cybercriminals were removed.

Experts estimate that approximately 75% of hacker attacks with "Petya" virus occurred in Ukraine, and in Poland, for example, only 5.81%. So how do they combat cybercrimes?

Firstly, changes were made to the legislation, which allowed proclaiming a state of emergency in the event of an attack in the virtual space.

Secondly, the Ministry of Administration and Digitalization was created, which task was to provide cyber security in the military sphere, protect the privacy of citizens, build a national educational platform, involving the elderly and residents of remote areas of the country.

Thirdly, the National Cybersecurity Center has been established. Its key task was to prevent threats, respond to them and coordinate actions.

Fourth, a new strategy for cybersecurity has been developed, which provides that by 2020 the authorities will ensure the safety of citizens, economic operators and state institutions in the field of cybersecurity.

Fifth, acknowledged the need for sufficient funding for cybersecurity measures.

We have Computer Emergency Response Team of Ukraine (CERT-UA), but in the United States there are 72 of such teams, in Germany - 23, in Poland - 2. So, there are structures, but their tasks are scattered, and the main body is not defined. In addition, these institutions employ too low skilled specialists with the appropriate salary level.

The situation with the law leaves much to be desired. We have the "Doctrine of Information Security", the Law on ratification of the Convention on Cybercrime, the Law on the basic principles of cybersecurity of Ukraine, the Decision of the National Security and Defense Council "On the strategy of cybersecurity of Ukraine". Legislative base is an important component, but if it remains on paper, the situation will not improve. It must be understood that there is no alternative to raising the level of cyber security.

Conclusions

On June 27, 2017, Ukraine was struck by the most powerful hacker attack for the whole history. The large-scale destructive attack of the attackers closed access to computers and computer networks in about 80% of Ukrainian enterprises (including foreign-owned companies).

The Department of Cyberpolicies of the National Police of Ukraine received more than 3,000 notifications of blocking computers.

The authorities began to investigate a serious computer attack. Several measures were taken to eliminate the threat and preventive measures were taken to protect non-contaminated systems.

We have encountered cyber attacks more than once. The most famous of them were attempts to intervene in the work of the CEC server in 2014, energy production companies' servers in 2016, as well as the sites of the State Treasury, the Ministry of Finance and other government agencies. But the Petya ransomware shows us that our state system of cyber security is still too weak. The path of Ukraine in this struggle is the need to improve the administrative legal system of cybersecurity, based on the experience of developed countries, close cooperation with them, as well as serious financial support.

Literature

Petya Ransomware Preliminary analysys CVE-2017-0199 + MS17-010. CERT-UA. 27/06/2017. New details about cyberattacks 27.06.2017 з використанням Petya ransomware. CERT-UA. 05 July 2017.

Michael Schmitt та Lieutenant Colonel Jeffrey Biller (11 липня 2017). The NotPetya Cyber Operation as a Case Study of International Law. Blog of the European Journal of International Law.

Constantin, Lucian. "Petya ransomware is now double the trouble".NetworkWorld

"Global ransomware attack causes chaos". BBC News. 27 June 2017.

Whittaker, Zack. "Six quick facts to know about today's global ransomware attack".ZDNet.