Revista Científica General José María Córdova
ISSN: 1900-6586
ISSN: 2500-7645
Escuela Militar de Cadetes "General José María Córdova"

Nizovtsev, Yuriy Yu.; Lyseiuk, Andrii M.; Kelman, Mykhailo
From self-affirmation to national security threat: analyzing the Ukraine's foreign experience in countering cyberattacks
Revista Científica General José María Córdova, vol. 20, no. 38, 2022, April-June, pp. 355-370
Escuela Militar de Cadetes "General José María Córdova"

DOI: https://doi.org/10.21830/19006586.905

Available in: https://www.redalyc.org/articulo.oa?id=476273700007

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

ISSN 1900-6586 (print), 2500-7645 (online)
Journal homepage: https://www.revistacientificaesmic.com

From self-affirmation to national security threat: analyzing the Ukraine's foreign experience in countering cyberattacks

Yuriy Yu. Nizovtsev
https://orcid.org/0000-0001-7398-0327
nizovtsev8218@sci-univ.com
Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine, Ukraine

Andrii M. Lyseiuk
https://orcid.org/0000-0002-1010-9566
lyseiuk8218@edu.cn.ua
Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine, Ukraine

Mykhailo Kelman
https://orcid.org/0000-0002-7414-984X
kelman8218@neu.com.de
National University, Ukraine

How to cite in APA: Nizovtsev, Y. Y., Lyseiuk, A. M., & Kelman, M. (2022). From self-affirmation to national security threat: analyzing the Ukraine's foreign experience in countering cyberattacks. *Revista Científica General José María Córdova*, *20*(38), 355-370. https://dx.doi.org/10.21830/19006586.905

Published online: April 1, 2022

Revista Científica General José María Córdova
(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 20, Number 38, April-June 2022, pp. 355-370
https://dx.doi.org/10.21830/19006586.905

From self-affirmation to national security threat: analyzing the Ukraine's foreign experience in countering cyberattacks

De la autoafirmación a la amenaza a la seguridad nacional: la experiencia Ucraniana y extranjera contra los ciberataques

Yuriy Yu. Nizovtsev and Andrii M. Lyseiuk
Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine, Ukraine

Mykhailo Kelman
National University, Ukraine

Abstract. This paper aims to study the main stages of cyberattacks' evolution in terms of the danger they pose, from the first hooligan cyberattacks to modern cyberwars. The authors use empirical qualitative and quantitative research methods to assess the stages of cyberattack development, considering their increasing numbers, diversity, and the creation of the malware employed. The paper provides a better understanding of the causes, conditions, and consequences of the emerging types of cyberattacks. The article concludes by pointing out the three stages in the evolution of cyberattacks and draws upon the main characteristic features of the current state of the cyber environment.

Keywords: critical infrastructure; cybercrime; cyber espionage; cyber terrorism; hacker groups; malware

Resumen. Este trabajo tiene como objetivo estudiar las principales etapas de la evolución de los ciberataques en cuanto a su peligrosidad, desde los primeros ciberataques gamberros hasta las ciberguerras modernas. Los autores utilizan métodos empíricos de investigación cualitativa y cuantitativa para evaluar las etapas del desarrollo de los ciberataques, teniendo en cuenta su incremento, su diversidad y la creación del malware empleado. El artículo permite comprender mejor las causas, las condiciones y las consecuencias de los nuevos tipos de ciberataques. El artículo concluye señalando las tres etapas de la evolución de los ciberataques y extrae los principales rasgos característicos del estado actual del ciberentorno.

Palabras clave: ciberdelincuencia; ciberespionaje; ciberterrorismo; grupos de hackers; infraestructuras críticas; malware

Section: Dossier • Scientific and technological research article

Received: November 30, 2021 • Accepted: March 6, 2022

Contact: Yuriy Yu. Nizovtsev ✉ nizovtsev8218@sci-univ.com

Introduction

Over the last few decades, information technologies have become especially developed and deeply integrated into almost all spheres of life, including entertainment, day-to-day life, production, finance, security, and defense. Naturally, criminals have not been oblivious to this progress in digital technologies, interfering in the work of automated information systems (cyberattacks) using various methods, including malicious software. The evolution of cyberattacks has advanced progressively, and the danger of these attacks has increased. The current scale of criminal acts in cyberspace has acquired the characteristics of real wars, providing a basis for considering these actions cyberwars by criminal hacker groups.

Scholars like Henley and Solon (2017), Denyer (2021), Von Neumann (1966), Hold (2010), Holovko (2017), Eaton and Volz (2021), Bakhur (2017), Parfylo (2016), and Woods and Weckler (2017), among others, have dedicated their works to the issues of countering cybercrime, including the investigation of crimes related to the use of malicious software. Nonetheless, the issues of cyberattacks' evolution still lack research. The increasing degree of their danger is a marked concern in modern studies.

There are several views on the origin of cyberattacks and how they have developed, including the use of malicious software. For example, some scholars consider that the first key stage began in December 1949, when John von Neumann (1966) gave a series of lectures at the University of Illinois on the *Theory and Organization of Complex Automata*. The materials of these and other lectures between 1948 and 1952 would form the basis of the theory of self-reproduction of automata and self-reproduction of certain classes of malicious programs. It was mainly students of North American universities who created the first malicious software, primarily distributing it through infected floppy disks (floppy disk drives). As a rule, these programs were created for research purposes or self-affirmation (hooligan motives). The best-known malware at the time included Brain, created in 1986; Lehigh, Stoned, and Jerusalem in 1987; the Morris Worm in 1988; and Michelangelo in 1991.

With time, cyberattacks began to acquire a commercial character, an illegal activity whose main purpose was for profit. Thus, a malware market emerged, where malware was sold or rented through specialized closed Internet resources. At the same time, the following types of malware were becoming increasingly widespread: extortionware, spyware, denial of service attacks software, adware, and spamware, among others. Recently, malware has begun to be used as a weapon (*cyber weapons*) in so-called cyberwars (Nuklearlord, 2012a), involving operations commonly referred to as cyberattacks or cyber diversions. The use of the malicious software, Stuxnet, is considered the first known case of cyber diversion (Nuklearlord, 2012b). Other software tools that appeared later, which accord-

ing to experts, can be attributed to *cyber weapons*, included Duqu, Wiper, Flame, Gauss, MiniFlame, Madi, Shamoon, and Narilam.

However, cyberattacks are no longer aimed at merely obtaining illegal material gains. Instead, they now aim to discredit specific firms or even country governments by exposing their alleged incompetence and weakness. The example here can be the cyberattack carried out by a Russian hacker group known as "Sandworm." This attack caused the world's first confirmed case of a power grid failure when the whole region was left without electricity (80 thousand households in total) (Inshyn et al., 2021).

New opportunities for criminal activity in the cyber environment, the increased intensity of cyberattacks, and the threats they pose to businesses and individual states' national security contribute to the relevance of the issue under research. This paper aims to analyze the main stages in the evolution of cyberattacks in terms of the danger they pose and better understand the causes, conditions, and consequences of the emerging types of cyberattacks.

Evolution of a cyberattack: analyzing the first and second stages

The first epidemic was caused by the Brain virus (also known as the Pakistani virus) in 1987. Its developers were the brothers, Amdjat and Basit Farooq Alvi. According to McAfee data, the virus has infected more than 18 thousand computers in the United States (The first article.., 1988). However, it did not perform destructive actions (Yefymenko, 2007); the program was written to determine the level of piracy in Pakistan. The virus infects the boot sectors, changes the disk label to *(c) Brain*, and leaves messages with the names, addresses, and telephone numbers of the authors. Its distinctive feature is the substitution of the infected sector with an uninfected original at the time of contact. Thus, the Brain can be called the first known stealth (invisible) virus. Within a few months, the program spread beyond Pakistan, and the epidemic reached global proportions by the summer of 1987.

The Lehigh virus was among the first destructive viruses. In 1987, it caused a mass infection of computers at Lehigh University (USA). Later, such phenomena would be called epidemics by analogy with biological viral diseases. The virus only infects the COMMAND.COM system files and is programmed to delete all the information on the current disk. The contents of hundreds of diskettes from the University library and students' personal diskettes were destroyed within a few days. All in all, about 4,000 computers were infected during the epidemic. However, Lehigh did not spread beyond the University (Novikovas et al., 2017).

The Suriv family of memory-resident file viruses, detected in 1987, was created by an unknown Israeli programmer. The most famous modification, Jerusalem, gave rise to

a global viral epidemic, the first real pandemic caused by an MS-DOS virus. Suriv viruses download code to a computer's memory, intercepting file operations and infecting COM and EXE files initiated by a user. This feature ensures the almost instantaneous spread of the virus on mobile data storage devices, at that time, floppy disks. Jerusalem differs from its predecessors by an additional destructive feature –the destruction of all running programs on Friday, the 13th. On the black date of May 13, 1988, the computers of many commercial firms, government agencies, and educational institutions, primarily in the United States, Europe, and the Middle East, became inoperable simultaneously.

On November 2, 1988, Robert Morris, a post-graduate student in the Department of Computer Science at Cornell University, released his worm. In less than a day, the worm spread to 6,000 machines –10% of the Internet at the time. It disabled many servers and users' computers connected to the network (Zobnin, 2015). This was the first case of mass infection via the Internet in history. The Morris Worm applied the following techniques simultaneously to penetrate 4BSD and Sun 3 systems: the Remote Shell Protocol (RSH), the sendmail email transfer agent, and the finger network protocol. The first one came into play when one of the users' passwords was cracked on the already infected machine; the worm would then try to use the same login and password on a remote machine. Infection via sendmail occurred by exploiting a vulnerability in the debug code. Simply connected to the server via SMTP, the worm would give the DEBUG command, pass the source code to its *head,* and the command to run and compile instead of the filling command in the FROM and DATA fields. The worm gained access to the system via finger due to a vulnerability in the gets function of the libc library, which was used by the daemon to read a request from a remote machine. The worm passed 536 bytes to the daemon, provoking a stack failure and transferring the shell code control.

In all three cases, the worm ran the netstat command, read the /etc/hosts file, and searched for neighboring machines on the network in other ways. It would then read the /etc/passwd file and its extracted password hashes and try to find passwords using an internal 432-word database, the /usr/dict/words file, and its own high-performance DES algorithm implementation. Then, the operation was repeated for other hosts. The total damage caused by the Morris Worm was estimated at $96.5 million. After confessing, Morris was sentenced to three years' probation, a fine of $10,000, and 400 hours of community service.

Launched in June 1994, OneHalf is a very complex resident file-loading polymorphic virus that caused a global epidemic, including in Ukraine. Depending on the modification, the OneHalf infects boot sectors of disks and COM/EXE files, increasing their size by 3544, 3577, or 3518 bytes. The last two unencrypted hard disk cylinders are encrypted each time the infected computer is restarted. This process continues until the entire drive is encrypted. The built-in stealth procedure allows the virus to decrypt on the

fly while requesting encrypted information. Consequently, the user will not notice anything suspicious for a long time. The only visual manifestation of the virus is the message, "Dis is one half. Press any key to continue..." This message is displayed on the screen when the number of encrypted disc cylinders reaches half their total number. However, when attempting to treat or after healing the disk's boot sectors, all the information on the disk becomes inaccessible and unrecoverable.

In June 1998, the Win95.CIH virus of Taiwanese origin was detected. It contains a logic bomb to destroy all information on hard drives and damage the BIOS contents on some motherboards. Because the program activation date (April 26) coincided with the date of the accident at the Chernobyl nuclear power plant, the virus received a second name, Chernobyl. The scale of the epidemic came to light on April 26, 1999, when according to various estimates, half a million computers worldwide were affected. The total damage was hundreds of millions of dollars. The epidemic center was South Korea, where more than 300,000 computers were infected.

After these first cyberattacks, this area of illegal activity was commercialized and used for profit. This change was followed by the emergence of a market for malware sold or rented, usually through specialized closed Internet resources. New centrally managed infected computers (so-called botnets) networks are also being sold or leased (Kozlovskyi et al., 2019). Moreover, extortionware, spyware, denial of service attacks software, adware, and spamware, among others, are becoming increasingly widespread.

Ransomware, on the other hand, blocks or significantly complicates the user's ability to work on the computer, requiring a ransom to unlock the computer. Currently, there are several radically different approaches to the work of extortionware, which involves file encryption in the system, blocking or interfering with the system's operation, and blocking or interfering with the Internet browser's work. Spyware is secretly installed on a user's computer, secretly transmitting certain types of information to its server. Spyware can serve a variety of purposes, both harmless and very dangerous (Antoniuk et al., 2018). An example of the former can be collecting particular programs' statistics to transmit them to developers to improve these programs. The authors' example of very dangerous ones includes receiving payment card details and client bank login credentials and transmitting them to the server.

A Denial-of-Service attack (DoS attack) involves interfering with the work of automated information systems; a successful implementation leads to the complete or partial inability of the mentioned systems to perform their functions (provide declared services). If such an attack is implemented from several sources simultaneously, it is called a distributed attack (DDoS attack, Distributed Denial-of-Service). DoS attacks are usually carried out to make the attacked system's resources inaccessible to legitimate users. The predicted consequences of these attacks include the inability to make payments via the Internet, loss

of the attacked resource owner's image of the attacked hosting's owner, and replacing the blocked resource with a *fake* one. Business competitors often commit such actions to gain market advantage, or criminals to demand ransom to stop the attack.

Programs for remote DoS attacks can have a graphical interface and operate with the user's knowledge. The best-known program of this kind is LOIC, an acronym for Low Orbit Ion Cannon or low-orbit ion gun. However, the software secretly installed on an infected computer, becoming part of a botnet, is used more often. A botnet (robot and network) is a computer network consisting of several hosts with running bots –standalone software. Most often, a bot in a botnet is a malicious program secretly installed on the victim's computer, allowing an attacker to perform specific actions using an infected computer's resources (Levchenko & Britchenko, 2021). An infected computer itself is often called a bot. Bots are usually used for illegal activities such as sending spam, retrieving passwords on a remote system, DoS attacks, obtaining users' personal information, and stealing credit card numbers and passwords. Among the largest known botnets is BredoLab, created in 2009 with about 30,000,000 bots, and Mariposa, created in 2008 with 12,000,000 bots.

Adware (from ad or *advertisement*) operation displays advertising. In some cases, this advertising can be useful. For example, when the developer inserts an ad to the program for advertiser discounts, and the user receives the program for free. However, the advertising program is often installed on the computer without the user's permission, most often even without the user's knowledge. Sometimes, the advertising displayed is so intrusive that it interferes with the work on the computer. Spam is the mass distribution of advertising or other correspondence to people who have not expressed a desire to receive it. The term *spam primarily* refers to promotional emails. Specialized programs designed for mass email sending are usually used for spam mass mailing. However, it is impossible to separate the legal program intended for sending mail and the malicious program intended for sending spam, as the harmfulness of distribution is determined by the recipients' authorization of this distribution.

Recently, malware has begun to be used as a weapon (*cyber weapons*) in so-called cyberwars (Nuklearlord, 2012a), some of its operations commonly referred to as cyberattacks or cyber diversions. These publications' format does not provide the specific actions' exact criminal and legal qualifications; their designations (cyber-terrorist attack or cyber sabotage) are approximated. The use of Stuxnet malicious software is considered the first known case of cyber diversion (Nuklearlord, 2012b). In late September 2010, it was discovered that the Stuxnet virus had caused serious damage to Iran's nuclear program. Exploiting operating system vulnerabilities and the infamous *human factor*, Stuxnet successfully affected 1,368 out of 5,000 centrifuges at the Natanga uranium enrichment plant and disrupted the Bushehr nuclear power plant launch. The client is still unknown.

However, many experts consider the United States and Israel as the developers and implementers of this cyber diversion (Nuklearlord, 2012b; Khlapkovskyi, 2016; Holovko, 2017; Stuxnet virus delivers…, 2010). The perpetrator was a negligent Siemens employee who installed an infected flash drive in the workstation. The damage to Iran's nuclear facilities could be compared to an attack by the Israeli Air Force (Hold, 2010).

After accessing the control system of the uranium enrichment centrifuges, the Stuxnet malware changed the centrifuges' normal mode of operation. As a result, they were either accelerated to a critical speed or suddenly decelerated. However, the reading on the screen showed the operator a normal mode of centrifuge operation. Continuous work in these extreme conditions led to the rapid failure of several centrifuges. It should be objectively noted that some sources deny the effectiveness of Stuxnet's harmful effects (Stuxnet and Iran…, 2010).

In terms of applied technologies, Stuxnet is an extremely high-tech and original solution in which the human factor is minimized in its application. Its characteristic feature is a thorough check of the affected automated information system. If the system found is not the targeted, the malicious program self-destructs without causing any harm to the affected system. This feature is not typical of *common* malware, one of the reasons why intelligence agencies have considered developing Stuxnet. Several other software tools subsequently appeared, which, according to experts, can be considered *cyber weapons*, including Duqu, Wiper, Flame, Gauss, MiniFlame, Madi, Shamoon, and Narilam.

Cyberattacks, a threat to a state's national security: third-stage qualitative and quantitative study

According to the authors, greater attention was given to the world's first confirmed case of power grid failure resulting from a cyberattack in Ukraine in December, when the Ivano-Frankivsk region was left without electricity (80 thousand households) due to outside interference in the operation of power grid facilities (Hubenko, 2016). The Security Service of Ukraine reported the detection of malicious software in the computer networks of some oblenergos (Prykarpattiaoblenergo, Kyivoblenergo, and Chernivtsioblenergo), accusing Russian criminal hacker groups of its distribution (SBU Press Service, 2015). Experts from US government agencies (State Department, Department of Energy, Department of Homeland Security, and the FBI) later joined the investigation, confirming the involvement of Russian hackers in the information attack (Perez, 2016). It was found that BlackEnergy malware was used in the attack carried out by a Russian hacker group known as *Sandworm*. Altogether, the cyberattack consisted of five elements: infecting networks with fake emails; obtaining control of the automated control system by disabling substations; decommissioning uninterruptible power supplies, modems, switchboards, and oth-

er IT infrastructure; destroying information on servers and workstations (using KillDisk utility); and attacking through call center telephone numbers (from Russian numbers) to deny energy services to subscribers (Interfax Ukraine, 2016).

On June 27, 2017, an unknown malware attacked many private and public companies in Ukraine, including banks (Cyberattack in Ukraine…, 2017). On that day, the National Bank of Ukraine warned other banks and financial sector industries about an external hacker attack by an unknown virus on several Ukrainian banks and some enterprises of the commercial and public sectors (National Bank of Ukraine, 2017). According to Microsoft, a total of 12.5 thousand computers in the country were affected by the virus (Microsoft Defender Security Research Team, 2017). Among the affected organizations were the Ukrzaliznytsia, Boryspil International Airport, Kyiv International Airport (Zhuliany), Epicenter, Nova Poshta, DTEK, Ukrenergo, Kyivenergo, Kyivvodokanal, Kyiv Metro, Antonov state enterprise, Document state enterprise, all national GSM mobile operators (Lifecell, Kyivstar, and Vodafone Ukraine), banks (Oschadbank, Ukrsotsbank, Ukrgasbank), and many others. State bodies also suffered an attack, particularly the Ukrainian Cabinet of Ministers and Ministry of Finance, and the website of the Lviv City Council, among others (Zakharov, 2017).

On the evening of May 27, 2017, the Cyber Police Department of the National Police of Ukraine published that *M.E.doc.* software (for reporting and document management) updates were used to spread the NotPetya malware (Parfylo, 2016; Cyberpolice…, 2017). This information was later confirmed by experts from the ESET anti-virus laboratory (Bakhur, 2017), Cisco Talos (Chiu, 2017), and Microsoft (Microsoft Defender Security Research Team, 2017). It should be noted that a month before the described events, the Cyberpolice Department warned the *M.E.doc.* program developers about their system's existing vulnerabilities, but the latter did not respond (Channel 24, 2017). *M.E.doc.* Software is widely used for document circulation and reporting in Ukraine. This explains the extremely fast and massive spread of NotPetya malware on the computers of Ukrainian organizations. According to ESET, almost 80% of all NotPetya virus infections occur in Ukraine (Bakhur, 2017). It should be noted that the update server of the *M.E.doc.* Program was hosted by the WNet Internet provider (Medium.com, 2017), whose unreliability in terms of information security was reported by the SSU shortly before the described events (Security Service of Ukraine, 2017; Kapustynska, 2017).

Specialists from the Kaspersky Lab (Ivanov & Mamedov, 2017) and Comae Technologies researcher Matt Suiche (2017) have concluded that it is generally incorrect to call NotPetya a cryptographer. The fact is that this malware is essentially designed to destroy information. It is almost impossible to restore the affected data. This is not a mistake; it is the malware's authors' intention. Therefore, NotPetya should be called a Wiper.

In general, the cyberattack was conducted as follows. Having accessed the hosting of the *M.E.doc.* program update server, the attackers introduced the NotPetya malicious software into the next update package. During the M.E.doc. Program's automatic update, NotPetya malware was downloaded to the computers being updated. NotPetya encrypted the media (hard drives) on the affected computers blocking access to them.

At first glance, the NotPetya malware cyberattack looked like an attack by *ordinary* cybercriminals with selfish motives to make money by extortion. It was only during a thorough investigation involving both domestic and foreign experts that it was established that this cyberattack was, in fact, large-scale cyber sabotage or cyberattack planned and carried out by a criminal hacker group (or association of such groups). It is important to consider the algorithm of operation of this malicious software in more detail.

Once on the computer, the NotPetya malware determines whether Kaspersky, Norton, or Symantec antivirus is running, disabling the antivirus when detected. After identifying and disabling the antivirus, NotPetya encrypts the data on the disk (files with the extension 3ds, 7z, accdb, ai, Asp, Aspx, avhd, back, bak, c, cfg, conf, cpp, cs, ctl, dbf, Disk, djvu, doc, docx, dwg, eml, fdb, gz, h, hdd, kdbx, mail, mdb, msg, nrg, ora, ost, ova, ovf, pdf, php, pmf, ppt, pptx, pst, pvi, py, pyc, rar, rtf, sln, sql, tar, vbox, vbs, vcb, vdi, vfd, and vmc). Then, it deletes the MBR (the original MBR is stored in the 0x22 disk sector and is encrypted using the XOR bitwise operation encoding *with* key *0x7*) and cleans the logs to hide traces of its actions as much as possible (Nesterenko, 2017). If the process has administrative privileges in the operating system, then, before replacing the MBR, the encryptor checks for the file called perfc (or another empty file with a different name) without extension in the directory C:\Windows\ (the directory is specified in the code). This file has the same name as the dll library of this encryptor, without the extension. The presence of such a file in the specified directory can be one of the indicators of compromise. If the file is present in this directory, then the malware execution process is completed (thus, creating a file with the correct name can prevent MBR substitution and further encryption). If the encryptor does not detect such a file during the check, the file is created, and the process of executing malicious software is started. This action is probably to prevent the MBR replacement process from restarting. On the other hand, if the process does not have administrative privileges from the very beginning, the encryptor will not be able to check for an empty file in the C:\Windows\ directory, and the file encryption process will still start without replacing the MBR and restarting the computer.

After starting the malicious file, a task to restart the computer with a 1 to 2-hour delay is created. Thus, there is time to run the bootrec / fixMbr command to restore the MBR and the operating system. Accordingly, it is possible to start the system even after it has been compromised, but it will not be possible to decode the files. A unique

AES key is generated for each disk, which remains in the memory until encryption is complete. Then, it is encrypted on the RSA public key and deleted. Recovering content after completion requires knowledge of the private key, without which it is impossible to recover data. The malware likely encrypts files to a maximum depth of 15 directories; files at greater depths are secure. If the disks were successfully encrypted after the reboot, a window with a message asking to pay a ransom of $ 300 (as of June 27, 2017, approximately 0.123 bitcoins) to obtain the key to unlock the files is displayed. Bitcoin wallet 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX is specified for money transfer.

NotPetya uses TCP ports 135, 139, and 445 (using SMB and WMI services) to spread. Spreading to other hosts on a network occurs in several ways. They include Windows Management Instrumentation (WMI), PsExec, and the MS17-010 (EternalBlue) vulnerability exploit. WMI is a technology to manage and monitor different parts of the Windows-based infrastructure centrally. PsExec is widely used for Windows administration and allows running processes on remote systems. However, running these utilities on the victim's computer requires local administrator privileges, which means that NotPetya can spread only from computers on which users have maximum operating system privileges. The EternalBlue exploit enables maximum privileges on an affected system. The encryptor also uses the publicly available Mimikatz utility to obtain credentials of all Windows users in plaintext, including local administrators and domain users. This toolkit allows NotPetya to spread even in infrastructures where the lessons of WannaCry were considered. This feature makes the encryptor very effective (Everything that you…, 2017).

NotPetya possesses functionality that allows it to spread to other computers in an avalanche-like process. It enables the encryptor to compromise the domain controller and attain control over all domain nodes, which fully compromises infrastructure. It should be noted that the NotPetya attack was not limited to Ukraine. Other countries also suffered huge losses. The malware has been used in Germany (9.06% of attacks), Poland (5.81%), Serbia (2.87%), Greece (1.39%), and Romania (1.02%). In Russia and the Czech Republic, it has accounted for less than one percent of all virus attacks (Stogniy, 2017). In the Russian Federation, the computers of Rosneft (NTV, 2017) and Bashneft (Russia was attacked…, 2017) stopped working almost simultaneously with Ukraine, resulting in the cessation of oil production at several sites.

Following Ukraine and Russia, attacks on networks began to be carried out in Spain, India (Griffin, 2017), Ireland, Great Britain (Woods & Weckler, 2017), and other countries and cities of the EU and the USA (Henley & Solon, 2017). According to Mcafee, more infected computers were recorded in the United States than in Ukraine. However, ESET (2017) antivirus statistics show that the highest number of recorded infections occurred in Ukraine.

On December 13, 2020, the information about a large-scale cyberattack against thousands of governmental and non-governmental institutions in the United States was released. The cyberattack began no later than March of that year. The attackers exploited software vulnerabilities of at least three software developers in the United States, including Microsoft, SolarWinds, and Vmware (Menn, 2020; Krebs, 2020). A supply chain attack on Microsoft cloud service provided attackers with a way to hack victims, depending on whether the services were purchased from an intermediary. The supply chain attack also struck the users of Orion *SolarWinds* IT *monitoring* and *management* tools, widely used by the U.S. Government and industry. Microsoft software vulnerabilities and VMWare allowed attackers to access emails and other documents to perform federated authentication of victims' resources using *Single Sign*-On (*SSO*) technology (Cimpanu, 2020).

The attackers embedded their own module (FireEye experts called it "Sunburst") in the Orion system, which opened a *backdoor* to the victims' computer networks (Goodin, 2020). Up to 200 organizations around the world were attacked. Most of them were US Government agencies and American companies; however, NATO, the UK Parliament, and the European Parliament were also affected (Gallagher & Donaldson, 2020).

On May 7, 2021, Colonial Pipeline, an American oil pipeline system, suffered a cyberattack, which shut down all its pipelines (Bing & Kelly, 2021). Given the scale of the cyberattack, the *President* of the *United States,* Joe Biden, declared a state of emergency (Suderman & Tucker, 2021). The Colonial Pipeline system delivers gasoline, diesel, and avgas from Texas to New York. This pipeline network supplies ~ 45% of the fuel consumed on the east coast of the United States. The attack came amid growing concerns about the infrastructure's vulnerability to cyberattacks, revealed after several high-profile attacks, including the hacking of SolarWinds in 2020, which affected several government agencies, including the Pentagon, the *Department of the* Treasury, the *Department* of *State,* and the Department of Homeland Security.

On May 6, within hours of the attack, the company paid hackers five million in cryptocurrency to restore operations. After the payment, the hackers gave the operator a data decoder. However, it was very slow, and the company had to use its own backups. A state of emergency was declared on May 9, 2021, due to a pipeline shutdown. The fuel tanks' supply was arranged, but their capacity was insufficient. A regional emergency was declared for 17 states and Washington, D.C. Moreover, the Federal Government lightened traffic of motorized transportation on highways to stabilize fuel supplies from Texas. By May 12, the Colonial Pipeline website was down. On May 13, the pipeline resumed operations; however, it took several days for the company to return to standard operation. On May 19, company representatives confirmed the payment to hackers. According to the CEO, Joseph Blount, the company paid them $ 4.4 million (Eaton &

Volz, 2021). The U.S. Department of Justice eventually recovered most of the ransom (Mallin & Barr, 2021).

Cyberattacks should also be considered against the backdrop of the COVID-19 global pandemic. For example, according to South Korean intelligence services, in 2021, hackers from the Democratic People's Republic of Korea (DPRK) attacked the Pfizer pharmaceutical company to steal confidential information concerning vaccines. They also stated that the number of cybercrimes from Pyongyang had increased by 32% over the past year. North Korea has not yet reported a single case of coronavirus in the country. In 2020 alone, North Korean criminals tried to reach at least nine medical organizations, including Johnson & Johnson, Novavax Inc., and AstraZeneca (Denyer, 2021).

Hackers from China also demonstrate considerable activity. The main area of their activity remains cyber espionage. Accordingly, in 2021, Chinese hackers *hacked* the Microsoft email service. It was established that the target included the data of research centers for the study of infectious diseases, law firms, universities, and companies. In addition, small businesses, municipal governments in several cities, and local governments were also affected, with a total of more than 20,000 organizations in the United States and tens of thousands worldwide. Microsoft claims that the cyberattack was probably carried out by attackers from China (BBC News, 2021).

Conclusion

The authors conclude that the danger of cyberattacks increases over time due to the anticipated attack results, the intensive integration of information technology into various spheres of life, and the possibility of influencing these areas through information technology.

The evolution of cyberattacks can be divided into three stages. In the first stage, cyberattacks were not directed against something or someone specific. They either did not have destructive functions, or these functions were insignificant and usually limited to data deletion. The purpose of those first cyberattacks was usually research or the desire for self-affirmation (hooligan motives). The emergence of specific cyberattack targets (Internet banking client apps and bank card payment data, among others) characterized the second stage. The very purpose of cyberattacks acquired clear selfish motives, resulting in significant financial losses. Cyberattacks were actually becoming a kind of criminal business.

The third stage is considered the most dangerous. The current state of global implementation of computer technology creates new opportunities for criminal activity in the cyber environment. As a result, the intensity of cyberattacks has increased significantly. Five to 10 years ago, casual hacker attacks for illegal enrichment were common.

Nowadays, the subject of discussion is true cyberwars by criminal hacker groups. The purpose of cyberattacks is no longer limited to simply obtaining direct illegal material benefits.

Often the purpose of a cyberattack is to discredit specific firms or entire countries (their governments) by revealing their alleged incompetence and weakness. The objects of cyberattacks can be critical infrastructure enterprises, whose shutdown would be critical on a national scale. On a regional or even global scale, the incident can potentially lead to man-made environmental disasters whose consequences can be compared with the Chernobyl disaster (with numerous casualties and significant material losses).

Thus, the danger of modern cyberwars of criminal hacker groups poses a threat not only to small, medium, and large businesses but also to the national security of individual states or even the security of the international community as a whole. It should be noted that cybercrime has no borders, and it is possible to combat it only by joining the efforts of law enforcement agencies and special services of all developed countries.

Disclaimer

The authors declare no potential conflict of interest related to the article.

Funding

The authors do not report sources of funding for this article.

About the authors

Yuriy Yu. Nizovtsev has a Ph.D. in Law. He is a Leading Researcher at the Research Laboratory of the Center for Forensic and Special Expertise Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine. He researches cyber wars, cyber security, and the cyber environment.

https://orcid.org/0000-0001-7398-0327 - Contact: nizovtsev8218@sci-univ.com

Andrii M. Lyseiuk has a Ph.D. in Law. He is an Associate Professor at the Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine. He has authored approximately 50 scientific works. His research interests include cyberattacks, national security, and forensic expertise.

https://orcid.org/0000-0002-1010-9566 - Contact: lyseiuk8218@edu.cn.ua

Mykhailo Kelman has a Ph.D. in Legal Science. He is a Professor at the Department of Educational and Scientific Institute of Law and Psychology Lviv Polytechnic National University, Ukraine. His research interests include countering cybercrime, international security, and human law.

https://orcid.org/0000-0002-7414-984X - Contact: kelman8218@neu.com.de

References

Antoniuk, L., Britchenko, I., Polishchuk, Y., Rudyk, N., Sybirianska, Y., & Machashchik, P. (2018). Code of ethics for SMEs: Substantiating the necessity and willingness to implement in Ukraine. *Problems and Perspectives in Management, 16*(3), 150-162. https://doi.org/10.21511/ppm.16(3).2018.12

Bakhur, V. (2017, June 28). *ESET: the source of the Petya.C outbreak was the compromised M.E.Doc*. C-News. https://safe.cnews.ru/news/line/2017-06-28_eset_istochnikom_epidemii_shifratora_petyac_stalo

BBC News. (2021, March 6). *Chinese Hackers Hacked Microsoft's Email Service. White House says Thousands of Organizations Remain at risk*. https://www.bbc.com/russian/news-56309038

Bing, C., & Kelly, S. (2021, May 27). *Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed*. Reuters. https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

Channel 24. (2017, July 5). *The police explained why the Petya.A virus was spread through M.E.Doc*. 24tv. https://24tv.ua/ru/v_policii_objasnili_pochemu_virus_petyaa_rasprostranili_imenno_cherez_medoc_n837954

Chiu, A. (2017, June 27). New ransomware variant "Nyetya" compromises systems worldwide. *Cisco Talos Intelligence*. https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html

Cimpanu, C. (2020, December 18). *NSA warns of federated login abuse for local-to-cloud attacks*. ZDNet. https://www.zdnet.com/article/nsa-warns-of-federated-login-abuse-for-local-to-cloud-attacks/

Cyberattack in Ukraine. Chronicle is completed. (2017, June 29). Ligue.Business. http://biz.liga.net/all/it/novosti/3696331-v-ukraine-proiskhodit-globalnaya-kiberataka.htm

Cyberpolice: Infection with Petya is due to M.E.Doc. Electronic Document Management System. (2017, June 27). Gordonua.com. http://gordonua.com/ukr/news/localnews/-kiberpolitsija-zarazhennja-virusom-petya-stalosja-cherez-sistemu-elektronnogo-dokumentoobigu-m-e-doc-194997.html

Denyer, S. (2021, February 16). *North Korea tried to steal Pfizer Coronavirus Vaccine Information, South says*. Washington Post. https://www.washingtonpost.com/world/asia_pacific/north-korea-pfizer-coronavirus-vaccine-hack/2021/02/16/c09ec7fc-702e-11eb-8651-6d3091eac63f_story.html

Eaton, C., & Volz, D. (2021, May 19). *Colonial Pipeline CEO tells why he paid hackers a $4.4 million ransom*. The Wall Street Journal. https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

ESET. (2017, June 28). "Petya" Ransomware: What we know now. *ESET North America.* https://www.eset.com/us/about/newsroom/corporate-blog/petya-ransomware-what-we-know-now/

Everything that you Wanted to know about NotPetya but were Afraid to ask. (2017, June 28). Positive Technologies. https://www.ptsecurity.com/ru-ru/about/news/283092/

Gallagher, R., & Donaldson, K. (2020, December 14). *U.K. Government, NATO join U.S. in monitoring risk from hack*. BNN Bloomberg. https://ampvideo.bnnbloomberg.ca/u-k-government-nato-join-u-s-in-monitoring-risk-from-hack-1.1536398

Goodin, D. (2020, December 17). *SolarWinds hack that breached gov networks poses a "grave risk" to the nation*. arsTECHNICA. https://arstechnica.com/information-technology/2020/12/feds-warn-that-solarwinds-hackers-likely-used-other-ways-to-breach-networks/

Griffin, A. (2017, June 27). *Huge 'Petya' cyber attack spreading across the world in potential repeat of 'Wannacry' hack.* Independent. https://www.independent.co.uk/life-style/gadgets-and-tech/news/hack-cyber-attack-ukraine-russia-wannacry-petya-security-internet-broken-computer-not-working-a7810626.html

Henley, J., & Solon, O. (2017, June 27). *'Petya' ransomware attack strikes companies across Europe and US*. The Guardian. https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe

Hold, R. (2010, October 11). *The virus that attacked Iran's nuclear facilities marked the beginning of the era of cyber warfare. Is the world on the brink of an IT military revolution?* Stuxnet: War 2.0. https://habr.com/ru/post/105964/

Holovko, V. (2017). Cyberattacks: Stuxnet Saboteur Virus in Nuclear Power Program of Iran. *Science and Technology, 128*(2), 33-41. https://naukatehnika.com/kiberataki-virus-diversant-stuxnet-v-yadernoj-energeticheskoj-programme-irana-chast1.html

Hubenko, D. (2016). *After the cyberattack on "Prykarpattiaoblenergo," the US Revises the Protection of Energy Grids*. Deutsche Welle. https://p.dw.com/p/1HZXJ

Inshyn, M., Khutoryan, N., Cherneha, R., Bontlab, V., & Tkachenko, D. (2021). Correlation of labor and civil contracts related to the performance of work: Preventing the substitution of concepts. *Employee Responsibilities and Rights Journal, 33*(4), 265-279. https://doi.org/10.1007/s10672-021-09373-3

Interfax Ukraine. (2016, February 12). *The Ministry of Energy Told the Details of the Cyberattack of the Russian Federation*. InfoResist. https://inforesist.org/v-minenergo-rasskazali-podrobnosti-kiberataki-rf/

Ivanov, A., & Mamedov, O. (2017, June 28). *ExPetr/Petya/NotPetya is a Wiper, Not Ransomware*. Securelist by Kaspersky. https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/

Kapustynska, K. (2017, June 1). *SBU summed up the searches in Wnet: The Provider Cooperated with the Russian Special Services*. Ukraine Segodnya. https://ukraine.segodnya.ua/ukraine/sbu-podytozhila-obyski-v-wnet-provayder-sotrudnichal-s-rossiyskimi-specsluzhbami-1026305.html

Khlapkovskyi, V. (2016, February 18). *Hack an entire country. Stuxnet virus was part of the US Plan to attack Iran*. rus.DELVI.lv. https://rus.delfi.lv/techlife/detali/vzlomat-celuyu-stranu-virus-stuxnet-okazalsya-chastyu-plana-ssha-po-kibernapadeniyu-na-iran.d?id=47076733

Kozlovskyi, S., Butyrskyi, A., Poliakov, B., Bobkova, A., Lavrov, R., & Ivanyuta, N. (2019). Management and comprehensive assessment of the probability of bankruptcy of Ukrainian enterprises based on the methods of fuzzy sets theory. *Problems and Perspectives in Management, 17*(3), 370-381. https://doi.org/10.21511/ppm.17(3).2019.30

Krebs, B. (2020, December 18). VMware Flaw a Vector in Solarwinds Breach? *Krebs on Security*. https://krebsonsecurity.com/2020/12/vmware-flaw-a-vector-in-solarwinds-breach/

Levchenko, I., & Britchenko, I. (2021). Estimation of state financial support for non-priority territorial units using the example of bridge construction. *Eastern-European Journal of Enterprise Technologies, 1*, 26-34. https://doi.org/10.15587/1729-4061.2021.225524

Mallin, A., & Barr, L. (2021, June 7). *DOJ Seizes millions in ransom paid by Colonial Pipeline*. ABCnews. https://abcnews.go.com/Politics/doj-seizes-millions-ransom-paid-colonial-pipeline/story?id=78135821

Medium.com. (2017, June 29). *M.E.Doc. Update Servers were Hosted by WNet*. Internetua. http://internetua.com/serveri-obnovlenii-M-E-Doc-okazalis-na-hostinge-WNet

Menn, J. (2020, December 17). *Microsoft Says it Found Malicious Software in its Systems*. Reuters. https://www.reuters.com/article/uk-usa-cyber-breach-idUKKBN28R3B7

Microsoft Defender Security Research Team. (2017, June 27). New Ransomware, old Techniques: Petya adds worm capabilities. *Microsoft Security*. https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/

National Bank of Ukraine. (2017, 27 June). NBU warned banks and other financial sector participants about external hacker attack. https://bank.gov.ua/ua/news/all/nbu-poperediv-banki-ta-inshih-uchasnikiv-finansovogo-sektoru-pro-zovnishnyu-hakersku-ataku

Nesterenko, S. (2017). *The secret of the Petya A virus has been revealed: it is a cyber weapon*. Code analysis. Personal website of Sergii NESTERENKO. https://sergnesterenko.com.ua/ru/tajna-virusa-petya-raskryta-eto-kiberoruzhie-analiz-koda/

Novikovas, A., Novikoviene, L., Shapoval, R., & Solntseva, K. (2017). The peculiarities of motivation and organization of civil defence service in Lithuania and Ukraine. *Journal of Security and Sustainability Issues, 7*(2), 369-380. https://doi.org/10.9770/jssi.2017.7.2(16)

NTV [@ntv.ru]. (2017, June 27) *Powerful attack: A Clone of the WannaCry Virus Spread on Rosneft's Servers* [video]. NTV. https://www.ntv.ru/novosti/1827659/

Nuklearlord (2012a, December 1). *Cyberwar – Stuxnet, Duqu, Flame, Gauss, and all, all, all...* [Online forum post] The Habr. https://habrahabr.ru/post/160973/

Nuklearlord. (2012b, November 17). *Again, about Stuxnet* [Online forum post]. The Habr. https://habrahabr.ru/post/159053/

Parfylo, O.A. (2016). Current Issues of Forensic and Expert Examination of Malicious Software Devices Within the Framework of the Fight Against Cyberterrorism. *Forensic Bulletin, 1*(25), 78-84. http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/krvis_2016_1_15.pdf

Perez, E. (2016, February 12). *U.S. official blames Russia for power grid attack in Ukraine*. CNN politics. https://edition.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/index.html

Russia was attacked by the same computer virus as Ukraine. (2017, June 27). iPress.ua. https://ipress.ua/news/rosiyu_atakuvav_takyy_zhe_kompyuternyy_virus_yak_i_ukrainu_216370.html

SBU Press Service. (2015, 28 December). *Security Service of Ukraine prevented an attempt by Russian Special Services to disable energy facilities in Ukraine*. Economical Truth. https://www.epravda.com.ua/news/2015/12/28/574276/

Security Service of Ukraine. (2017). SBU Exposed the Ukrainian Internet Provider on Illegal Traffic Routing to Crimea in the Interests of Russian Special Services. https://www.sbu.gov.ua/ru/news/134/category/78/view/3451#.zxQtepPG.dpbs

Stogniy, K. (2017, June 30). *Files cannot be retrieved after a Petya virus attack – experts*. Nnovosti.info. https://nnovosti.info/news/vidnoviti_fajli_pislja_ataki_virusu_petya_nemozhlivo_eksperti-18483.html

Stuxnet and Iran: The Mystery of the A26 module. (2010, December 30). Atomic Energy. https://www.atomic-energy.ru/articles/2015/05/06/17237

Stuxnet Virus Delivers Devastating Blow to Iran's Nuclear Program. (2010, December 16). SecurityLab.ru. http://www.securitylab.ru/news/402905.php

Suderman, A., & Tucker, E. (2021, May 8). *Major US pipeline halts operations after ransomware attack*. AP News. https://apnews.com/article/ga-state-wire-business-c6ef4314af911fb58b8445d2b121e82d

Suiche, M. (2017, June 28). *Petya.2017 is a wiper not a ransomware*. Comae Technologies. https://medium.com/comae/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b

The First Article about Viruses in Russian. (1988, July 26). SecurityLab.ru. http://www.securitylab.ru/former/240714.php

Von Neumann, J. (1966). *Theory of self-reproducing automata.* Completed by Burks, A. W. (Ed.). Urbana and London: University of Illinois Press.

Woods, B., & Weckler, A. (2017, June 27). *Global cyber attack hits IT systems in Ireland and the UK*. Independent.ie. https://www.independent.ie/business/technology/global-cyber-attack-hits-it-systems-in-ireland-and-the-uk-35871179.html

Yefymenko, V. (2007). *Information security management: Viruses and countermeasures.* Saint Petersburg: National Open University "INTUIT."

Zakharov, D. (2017, June 27). Banks and companies that suffered from the cyberattack: A list. ZN.UA. https://zn.ua/ukr/UKRAINE/banki-ta-kompaniyi-scho-postrazhdali-vid-kiberataki-perelik-246826_.html

Zobnin, Ye. (2015). Infectious penguins. The history of program virus writing for *nix systems in numbers. https://xakep.ru/2015/10/20/nix-viruses-history/